Dunakavics

A Dunaújvárosi Egyetem online folyóirata 2020. VIII. évfolyam III. szám

Műszaki-, Informatikai és Társadalomtudományok

Csiszár Csaba–Földes Dávid –Csonka Bálint
A közlekedési informatika oktatása a BME Közlekedésüzemi és Közlekedésgazdasági tanszékén

Szakács Balázs
Biztonságtudatos informatikai eszközhasználat 1. rész

Kovács István Béla
Riesz-terek típusairól röviden

Imre E.–Barreto, D.–Talata I.–Baille, W.–Rahemi, N.–Goudarzy, M.–Lőrincz J.–Singh, V. P.
Grading curves and internal stability

Oroszi Eszter Diána
Biztonságtudatossági szabadulószoba, mint új programelem az információbiztonsági képzésekben



Dunakavics

A Dunaújvárosi Egyetem online folyóirata 2020. VIII. évfolyam III. szám

Műszaki-, Informatikai és Társadalomtudományok

Megjelelenik évente 12 alkalommal

Szerkesztőbizottság

András István, Bacsa-Bán Anetta, Balázs László, Nagy András
Nagy Bálint, Németh István, Rajcsányi-Molnár Mónika.

Felelős szerkesztő Németh István
Tördelés Duma Attila

Szerkesztőség és a kiadó címe 2400 Dunaújváros, Táncsics M. u. 1/a.

Kiadja DUE Press, a Dunaújvárosi Egyetem kiadója
Felelős kiadó Dr. habil András István, rektor

A lap megjelenését támogatta a Nemzeti Kulturális Alap

TÁMOP-4.2.3-12/1/KONV-2012-0051
„Tudományos eredmények elismerése és disszeminációja
a Dunaújvárosi Főiskolán”.
http://dunakavics.due.hu
ISSN 2064-5007

Tartalom

CSISZÁR CSABA–FÖLDES DÁVID–CSONKA BÁLINT

A közlekedési informatika oktatása a BME Közlekedésüzemi és Közlekedésgazdasági tanszékén 5

SZAKÁCS BALÁZS

Biztonságtudatos informatikai eszközhasználat 1.rész 15

KOVÁCS ISTVÁN BÉLA

Riesz-terek típusairól röviden 29

IMRE E.–BARRETO, D.–TALATA I.– BAILLE, W.–RAHEMI, N.–GOUDARZY, M.–LŐRINCZ J.–SINGH, V. P.

Grading curves and internal stability 37

OROSZI ESZTER DIÁNA

Biztonságtudatossági szabadulószoba, mint új programelem az információbiztonsági képzésekben 51

Galéria 63

(Bakos Miklós fotói)



CSISZÁR CSABA *–FÖLDES DÁVID **–CSONKA BÁLINT ***

A közlekedési informatika oktatása a BME Közlekedésüzemi és Közlekedésgazdasági tanszékén

Összefoglalás: A közlekedés egy összetett rendszer; a közlekedési szervezetek és folyamatok szervezése, valamint célorientált működtetése egyre nagyobb méretű információ-halmazok kezelését jelenti. A közlekedési informatika fogalma és tárgyköre a múlt század második felétől kezdődően alakult ki és azóta is folyamatosan, egyre gyorsuló ütemben fejlődik. A kétlépcsős közlekedésmérnöki képzés (alap- és mesterképzés) része a közlekedési információs rendszerek megismerése és a közlekedési informatikai rendszerek tervezésének elméleti és gyakorlati tudásanyagának elsajátítása. A technikai és tudományos ismeretek bővülése miatt az oktatási anyag folyamatosan fejlődik, az elért eredmények tematikusan beépülnek az oktatásba. A cikkben a BME Közlekedésüzemi és Közlekedésgazdasági Tanszékén közlekedési informatika témakörben végzett elméleti és gyakorlati oktatást mutatjuk be.
Kulcsszavak: Adatbáziskezelés, adatmodell, folyamat, információ, integráció, közlekedési informatika, rendszer.

Abstract: Transport is a complex system; planning and goal-oriented operation of transport organizations and processes require management of large information sets. The term and subject of transport informatics have been used since second half of the last century and it is still in an uninterrupted and ever accelerating progress since then. The two-level (BSc, MSc) study program in transportation engineering includes theoretical and practical materials regarding transport information services and systems. Expansion of technical and scientific knowledge requires the widespread research of the topic and incorporation of the results into the education. In this paper, the theoretical and practical tuition of transport informatics at the Department of Transport Technology and Economics of the BME (Budapest University of Technology and Economics) is presented.
Keywords: Database management, data model, information, integration, process, transport informatics, system.

*Budapesti Műszaki és Gazdaságtudományi Egyetem, Közlekedésmérnöki és Járműmérnöki Kar
E-mail: csiszar.csaba@mail.bme.hu

**Budapesti Műszaki és Gazdaságtudományi Egyetem, Közlekedésmérnöki és Járműmérnöki Kar
E-mail: foldes.david@mail.bme.hu

***Budapesti Műszaki és Gazdaságtudományi Egyetem, Közlekedésmérnöki és Járműmérnöki Kar
E-mail: csonka.balint@mail.bme.hu

Bevezető

Az elmúlt évtizedek műszaki fejlődésének egyik meghatározó jelensége az automatizálás, a valós világ egyre részletesebb leképezése információkkal és az információk sokrétű felhasználása az aktuális körülmények egyre nagyobb mértékű figyelembevételével. Rohamosan fejlődik az adatok, információk térbeli gépi kezelésének technológiája; kialakult az a tudás, amely egész szervezetek információs rendszerének tervezéséhez, fejlesztéséhez szükséges.

Az informatika az információs rendszerek szerkezetét, működését és fejlesztését vizsgálja, a kommunikáció (kapcsolattartás) folyamatainak törvényszerűségeivel foglalkozik; lényegében az információk alkalmazása a társadalmi szükségletek kielégítésére. Definíció szerint az informatika: az információk rendszerszintű kezelésével összefüggő ismeretek összessége.

Technikai háttere az infokommunikációs eszköztár. Az informatika azon információk szisztematikus és hatékony kezelésének tudománya, amelyeket az emberi tudás és kommunikáció hordozójának tekintünk műszaki, gazdasági és társadalmi összefüggésekben. Mindezek alapján látható, hogy az informatika jóval több az egyes informatikai megoldások összességénél.

Az elméleti informatika jellegzetes tárgytartományai az információ- és programozás-elmélettel kapcsolatosak. A gyakorlati informatika a szervezetek, rendszerek elemeinek és működésének leképezésével, adatmodellezéssel, adatbázis-tervezéssel, gyakorlati programozással, az infokommunikációs rendszerek tervezésével, fejlesztésével foglalkozik.

A technikai informatika a számítógép-hálózatok szerkezetének vizsgálatára, tervezésére, fejlesztésére, működtetésére terjed ki. A három említett ismeretkör általános informatikának nevezhető. Az alkalmazott informatika megjelenik különböző tudományterületeken belül és ágazatokon belül, így a közlekedésben is, ahol a szervezetek teljes információellátásával kapcsolatos rendszerszemléletű megoldásokat jelenti.

A közlekedési rendszerek tervezése és működtetése a technológiai, szervezési, üzemeltetési, gazdasági és jogi ismeretanyagok mellett egyre inkább igényli az információkezeléssel összefüggő ismereteket is. A közlekedési mérnöki képzés során a hangsúly az elméleti és gyakorlati informatika területén elérhető tudás megszerzésére helyezzük. A téma jelentőségét a napjainkban megfigyelhető, hosszabb folyamatként tekinthető ún. információrobbanás fokozza.

A kezelt információ mennyiségét alapvetően a közlekedésben résztvevő alapfolyamati összetevők száma, az egyes összetevőkről gyűjtött jellemzők köre és a mintavételezési időköz befolyásolja. Az utóbbi két tényező miatt az utóbbi időszakban jelentősen nőtt a kezelendő adatok mennyisége, miközben a felhasználás során továbbra is kis időtartam áll rendelkezésre a lekérdezések lefuttatására.

További kihívás a különböző forrásokból származó, eltérő formátumú, jelentéstartalmú, stb. információ „összefésülése" és „közös kezelése", ami a közlekedés egész információs rendszerére kiterjedő integráció alapfeltétele.

A cikk további részében a BME Közlekedésüzemi és Közlekedésgazdasági Tanszékének informatika témájú oktatási tevékenységét foglaljuk össze, az elméleti és a gyakorlati képzésre összpontosítva.

Elméleti oktatás

A Tanszéken több évtizede folyik a közlekedési informatikával és rendszerekkel kapcsolatos oktatás. [1–5] Jelentős változás a kétszintű képzésre való áttéréskor történt. A korábbi *Közlekedési informatika* c. és *Közlekedési rendszertervezés* c. tárgyak ismeretanyagának tagolása átalakult. Az alapképzésben (BSc) az alkalmazott közlekedési informatikai ismeretanyagokat a *Közlekedési információs rendszerek I. és II.* c. tárgyak fedik le, míg a mesterképzésben (MSc) a *Közlekedési informatika* c. tárgy tartalmazza az információs rendszerek felépítését és működését leíró modelleket és a módszertani ismeretanyagokat.

A tárgyak tartalmába folyamatosan beépítjük az ismereti és technikai fejlődés legújabb eredményeit, és saját tudományos kutatási eredményeinket, miközben követjük az időtálló absztrakciós szinteket és csoportosítási elveket is.

Mivel a Karon külön tanszék foglalkozik a logisztika területével, így a Közlekedésüzemi és Közlekedésgazdasági Tanszéken a személyközlekedéssel összefüggő ismeretanyagok a hangsúlyosabbak. Az oktatott témaköröket az *1. táblázat* foglalja össze.

[1] Westsik Gy. (1989): *Közlekedési informatika.* Egyetemi tankönyv. Budapest: Tankönyvkiadó.

[2] Westsik Gy. (1994): *Közlekedési Informatika II.* (Alkalmazott közlekedési információtechnika). Budapest: Műegyetemi.

[3] Westsik Gy. (1995): *Közlekedési Informatika I.* (Általános közlekedési informatika). Budapest: Műegyetemi.

[4] Westsik Gy. (1995): *Közlekedési rendszertervezés.* Budapest: Műegyetemi.

[5] Munkácsiné Lengyel E.–Tóth J.–Csiszár Cs.–Juhász J. (2004): *Közlekedési informatika.* (Jegyzet). Budapest: Műegyetemi.

1. táblázat. A Közlekedési információs rendszerek I. és II. (BSc) c. tárgyak és a Közlekedési informatika (MSc) c. tárgy témakörei.

	Közlekedési információs rendszerek I.	**Közlekedési információs rendszerek II.**	**Közlekedési informatika**
1	Információs rendszerek alapismeretei	Az utasinformatika témaköréhez kapcsolódó alapfogalmak	A közlekedési informatika alapfogalmai (az informatikai szabályozókör)
2	Adatmodellezés	Menetrendi, díjszabási és turista információszolgáltatás	A közlekedési rendszer szerkezete (az információs rendszer elhelyezkedése)
3	Relációs adatmodell, adatbázis-tervezés	Helyfoglalás informatikája	Vázszerkezeti modell (elemszerkezet, elemeken belüli szerkezet)
4	Adatbázisok normalizálása	Számítógépes menetdíjbeszedés	Vázszerkezeti modell (az elemek közötti kapcsolati szerkezet, dinamikus szerkezet)
5	Számítógépes hálózatok felépítése, működése	Az utasbiztonság fokozása telematikai rendszerekkel	Szervezetek csoportosítása, szervezeti felépítés, tevékenységi szerkezet
6	Műholdas kommunikációs rendszerek	A járműhöz vezetés és a járműtől való elvezetés informatikája	Vezetési szintek funkciói és az információellátás jellemzői
7	Helymeghatározó rendszerek	Járműfedélzeti informatika	Dinamikus funkcionális (működési) modell
8	Járműkövető rendszerek	A személyszállítási informatika hardver megoldásai	A közlekedési szervezetek informatikai szerkezete
9	Intelligens közlekedési rendszerek (ITS) alapismeretei	Parkolási módok informatikai jellemzői; célok, funkciók	Modellezési módszerek (szempontrendszer, összetevők, modelltípusok, térbeli ábrázolás)
10	Kooperatív ITS rendszerek (C-ITS) alapismeretei	Integrált parkolásirányító rendszer felépítése, működése	Elemzési módszerek (szempontok, adatkezelési és adatáramlási elemzések, alkalmazási területek)
11	Gyalogos közlekedés információs rendszerei	Intermodális csomópontok informatikája	Az elektromos közúti járművek működési jellemzői; az elektromobilitási rendszer
12	Kerékpáros közlekedés információs rendszerei	Bookroad – a közúti útvonalfoglalás információs rendszere	Az elektromos közúti járművek töltőinfrastruktúrája
13	Közlekedési alágazatok össze-hasonlítása információs rendszerüket befolyásoló szempontok szerint	Telematikailag integrált személyközlekedés	Az elektromos közúti járművek töltésének szabályozása (smart grid)
14	Városi integrált információs rendszer	Az utazók információkezelési műveletei, a döntések befolyásolása	Az elektromobilitáshoz kapcsolódó információs rendszer és szolgáltatások
15	A vasúti közlekedés informatikai szabályozási struktúrája; az információs rendszerek csoportosítása	Az elektromobilitás üzemeltetési jellemzői, információkezelési jellemzők	Az autonóm járművek technológiája – alapfogalmak, típusok, működési jellemzők
16	A vasúti közlekedés jellegzetes információs rendszerei	Autonóm (önvezető) járművek információ-kezelési folyamatai	Az autonóm járművekre épített közlekedési rendszer és mobilitási szolgáltatások
17	A vízi közlekedés információs rendszerei	Autonóm közforgalmú közlekedés informatikája	Az autonóm járművekre épített mobilitási szolgáltatások tervezése, üzemeltetése
18	A légi közlekedési informatika alapjai	Smart city – Okos város Smart mobility – Okos közlekedés	Az autonóm járművek hatásai

Közlekedési információs rendszerek I. és II. tárgyak keretében a hallgatók megismerkednek az információval, információs rendszerekkel kapcsolatos fogalmakkal, szabályszerűségekkel, technológiákkal, alkalmazási területekkel és fejlesztési lehetőségekkel a közlekedés területén. Ennek megfelelően a tantárgy foglalkozik az intelligens közlekedési rendszerek és az okos városok (smart city) alapismereteivel is; mindkét esetben kitérve az alrendszerek kooperációjának jelentőségére. Továbbá az újszerű közlekedési rendszerek, úgy, mint az elektromobilitás és autonóm járműves mobilitás információkezelési folyamatai is a tantárgy részét képezik. Az általánosan alkalmazott informatikai megoldások mellett az egyes közlekedési alágazatok informatikai jellegzetességei a szállítási folyamat és a szervezeti jellemzők eltérései miatt különböznek. Az idők során az egyes alágazatok informatikai fejlődési intenzitása is eltéréseket mutatott. Ennek megfelelően összetett szempontrendszer szerint világítunk rá a hasonlóságokra és a különbözőségekre. A konkrét alkalmazott informatikai fejezetek a személyközlekedés megoldásaival foglalkoznak gyakorlatorientált megközelítésben. Az alkalmazások bemutatási rendje a helyváltoztatási módokra és a folyamatra fókuszál. A témakör az információs rendszerek integrációjának kérdéskörével zárul, mely egyben előrevetíti és összefoglalja a jövőbeli fejlődési irányokat is. A szakirányok választását követően a hallgatók külön tárgyak keretében mélyednek el az adott alágazat informatikai sajátosságaiban és az alkalmazott rendszerekben.

A Közlekedési informatika tárgy magasabb absztrakciós szinten világítja meg a rendszertervezés alapelveit és módszereit, elsősorban az információs rendszerekre helyezve a hangsúlyt. Fontos szempont volt, hogy az alapképzés során elsajátított közlekedési információs rendszerekkel, adatbázis-kezeléssel, technológiával, üzemeltetéssel kapcsolatos ismeretekre építve a hallgatók rendszer- és folyamatszemléletű tárgyalásban is átlássák a logikai összefüggéseket. Ez az absztrakció lehetőséget ad számukra, hogy a komplex információs rendszerek üzemeltetése mellett sikeresen részt vegyenek azok tervezésében, fejlesztésében is. A tantárgy a közlekedés alapfolyamatának lebonyolításában, illetve irányításában résztvevő rendszerösszetevők tevékenységéhez kapcsolódó információk rendszerbe foglalásával, és a közlekedési szervezetek információellátásának kérdésköreivel foglalkozik. Az eladások során a közlekedési információs rendszerek szerkezeti és működési modelljein keresztül a hallgatók megismerik a statikus és dinamikus jellemzőket, valamint a közlekedés és a mobilitási szolgáltatások tervezési, szervezési, irányítási és ellenőrzési folyamatának modellezését. Az utóbbi évek kutatási eredményeit az elektromobilitás és az autonóm járművekre épülő közlekedés rendszer területén is beépítettük az elméleti oktatásba.

A hallgatók felkészítését segítendő, 2018-ban a *Közeledési információs rendszerek I. és II.* tárgyakhoz jegyzetet készítettünk [6].

[6] Csiszár Cs.–Földes D.–Csonka B. (2018): *Közlekedési információs rendszerek.* Budapest: Akadémiai.

A közlekedési informatika tárggyal összefüggésben, az *Innovative Passenger Transportation System* c. angol nyelvű egyetemi könyv [7] használatával szerezhetnek a hallgatók további ismereteket.

Gyakorlati oktatás

A gyakorlati képzés során a hallgatók adatbáziskezelési, és az információs rendszerek tervezéséhez szükséges tudásra tesznek szert [5], [8], [9] gyakorlati oktatása. A tananyag fejlesztése folyamatos. A hallgatók alapképzésen a Közlekedési információs rendszerek I. és II. tárgyak keretében két félév során sajátítják el az adatmodellezés és adatbáziskezelő alkalmazások ismeretanyagát heti rendszerességű, kiscsoportos (kb. 20 fős) számítógépes gyakorlatok során. A közlekedési információs rendszerek legfontosabb „soft" összetevője az adat; a képzés során elsősorban a tárolási szerkezet és a feldolgozási műveletek megtervezésére helyezzük a hangsúlyt. Célunk, hogy az egyetemi képzésben szerzett „iskolai jellegű" feladatokon keresztül a hallgatók később eredményesen tudjanak bekapcsolódni összetettebb, nagyobb léptékű rendszertervezési és -fejlesztési feladatokba is, ahol ezek az alapismeretek és készségek nélkülözhetetlenek.

Első félévben az adatmodellekre és azok tervezésére helyezzük a hangsúlyt. Az adatbázis-kezelés ismeretköre a kifejlődés előzményeivel, alapjaival kezdődik. A fogalmakat és definícióikat, valamint azok egymásra épülését a hallgatók az előadásokon sajátítják el, amelyet a gyakorlati foglalkozások példáin keresztül mélyítenek el. A képzés során a hallgatók részletesen megismerkednek a relációs adatmodellezéssel, valamint az adatbáziskezelés elterjedt nyelvezetével (SQL – Structured Query Language) és annak használatával. A korábbi félévek tapasztalati alapján a hallgatók számára nehézséget okozott a fogalmi modellek értelmezése és a logikai modell elkészítése, főként az adattáblák normalizálása. A normalizálás (táblázat-szétbontó műveletek) során alakítjuk ki a „helyes" tárolási szerkezetet. Ezen nehézségek miatt kiemelt figyelmet fordítunk a logikai modell és a normalizálás gyakorlására. Az órán a hallgatók a gyakorlatvezető iránymutatásával mintafeladatokat oldanak meg, továbbá a félév során összesen hét otthoni szorgalmi feladatban gyakorolhatják a logikai modell készítését. Az SQL-nyelv használatával a hallgatók megtanulják az adatbázisok létrehozását, módosítását és különböző típusú lekérdezések készítését. Az SQL-nyelv megtanulásával a hallgatók eltérő szoftverkörnyezetben is magabiz-

[5] Munkácsiné Lengyel E.–Tóth J.–Csiszár Cs.–Juhász J. (2004): *Közlekedési informatika.* (jegyzet)

[7] Csiszár Cs.–Csonka B.–Földes D. (2019): *Innovative Passenger Transportation Systems.* Budapest: Akadémiai.

[8] Csiszár Cs.–Sándor Zs. (2014): *Közlekedési informatika.* (elektronikus egyetemi jegyzet)

[9] Csiszár Cs.–Westsik Gy. (2014): A közlekedési informatika kutatása és oktatása a BME Közlekedésüzemi és Közlekedésgazdasági tanszékén. *Közlekedéstudományi Szemle.* LXIV (2). Pp. 44–52.

tosan mozognak. A hallgatók egy választott közlekedési témában saját adatmodellt is készítenek féléves házifeladatként, mely során megfogalmazzák az adatok feldolgozásakor feltett kérdéseket és a megválaszolásukhoz szükséges SQL-parancsokat.

A második félév során a könnyen szerkeszthető és felhasználóbarát alkalmazások fejlesztéséhez szükséges ismeretanyag elsajátítása a cél. Így az adatok rendszerezéséhez szükséges lekérdezéseken túl, űrlapok és jelentések készítése is a tananyag része. Az űrlapok az adatoknak elektronikus felületen (monitor) történő kezelését teszik lehetővé, míg a jelentésekkel táblák és lekérdezések adatait tudjuk megjeleníteni áttekinthető és nyomtatásra kész formátumban. A hallgatók a félév során összetett alkalmazások fejlesztéséhez szükséges események és makrók szerkesztését is elsajátítják. A makró egy eszköz, mely lehetővé teszi a folyamatok automatikus végrehajtását. Továbbá, a hallgatók a félév során betekintést kapnak a Visual Basic programozás egyszerűsített változatába, amely segítségével szintén folyamatokat automatizálnak. A nagy adatbázis-kezelő rendszerek ma már hálózat-bázisúak, speciális jellemzőkkel (pl. jogosultsági szintekkel). A gyakorlatokon, a könnyű hozzáférhetőség érdekében, a Microsoft Access adatbázis-kezelő programot használjuk önálló (stand alone) üzemben. Ez a program számos beépített segédeszközzel (pl. varázslók) és felhasználóbarát grafikus felülettel teszi élvezetessé a használatot. Azonban az összetett feladatok algoritmusfejlesztési és programozási ismereteket is megkívánnak az SQL-nyelv ismerete mellett. A gyakorlati órákon való előrehaladás mellett a hallgatók folytatják az előző félévben kiválasztott feladatuk kidolgozását, működő alkalmazás fejlesztésével, amit dokumentálnak és a félév végén bemutatják az elért eredményeket.

A gyakorlati tananyag könnyebb elsajátítása érdekében elektronikus jegyzetet készítettünk az adatmodellezés [10] és az adatbáziskezelés [11] témakörökben. A jegyzetek fejezetei az órák tematikáját követik. A témaköröket az *2. táblázat* foglalja össze. Terjedelmi korlátok miatt a jegyzetek csak a tananyag vázát tartalmazzák, így azok tartalma évről-évre változhat. A parancsok kipróbálása, gyakorlati elsajátítása számítógépes laborban történik, ami megkívánja a hallgatóság laborfoglalkozásokon történő intenzív részvételét. A házi feladatok kidolgozása a gyakorlatvezetők folyamatos támogatásával zajlik. Ez a munkamódszer lehetővé teszi, hogy a hallgatók a speciális problémához illeszkedő ismereteket is összegyűjtsék, hiszen a laboratóriumi gyakorlatokon nincs lehetőség minden részletes ismeret átadására.

[10] Csiszár Cs.–Csonka B.–Földes D. (2018): *Közlekedési információs rendszerek I. - Számítógépes laborgyakorlat.* (elektronikus egyetemi jegyzet) Budapest: Akadémiai.

[11] Csiszár Cs.–Csonka B.–Földes D. (2018): Közlekedési információs rendszerek II. - Számítógépes laborgyakorlat. (elektronikus egyetemi jegyzet) Budapest: Akadémiai.

2. táblázat. A Közlekedési információs rendszerek I. és II. (BSc) c. tárgyak témakörei.

	Közlekedési információs rendszerek I.	**Közlekedési információs rendszerek II.**
1	Az adatbáziskezelés alapjai (adatmodellezés, adatmodellek típusai, adatbázis-kezelő szoftverek, SQL nyelv jellemzői, adattípusok)	A mintaadatbázis jellemzői (szerkezete, mezőtulajdonságok, kapcsolattípusok)
2	Normalizálás (példák. N:M kapcsolatok felbontása, kódtábla)	A mintaadatbázis létrehozása (táblaszerkezetek, megszorítások és alapértelmezett értékek, beviteli maszk, táblák összekapcsolása)
3	Mintaadatbázis létrehozása (szerkezet, minta adatok)	Lekérdezések I (választó, paraméteres, csoportképző, kereszttáblás)
4	SQL-parancsok csoportosítása, SELECT-parancs I (DDL, DML, SELECT-parancs szerkezete, rendezés)	Lekérdezések II (azonosakat kereső, akció-lekérdezések, függvények)
5	SELECT-parancs II (hiányzó adatelem, predikátumok, sorfeltétel, operátorok)	Űrlapok (űrlapok szerkezete, jellemzői, kötött és kötetlen vezérlőelemek, segédűrlap)
6	SELECT-parancs III (függvények, csoportképzés, csoportfeltétel)	Jelentések, események, makrók, adatbázis eszközök
7	Összetett lekérdezések (több táblás, egymásra épülő, beágyazott lekérdezése)	Visual Basic for Application (VBA) I (bevezetés a VBA nyelvezetbe, kódszerkezet, változók, konstansok, függvények deklarálása)
8	DDL-parancsok (CREATE, ALTER, DROP-parancsok, érvényességi szabály, alapértelmezett érték)	Visual Basic for Application (VBA) II (logikai elágazások, ciklusok)
9	DML-parancsok (INSERT INTO, UPDATE, DELETE FROM parancsok, unió, táblakészítő lekérdezés)	Alkalmazásfejlesztés, menürendszer
10	Gyakorlás – példafeladatok megoldása	Gyakorlás – példafeladatok megoldása

A mesterképzés során a Közlekedési informatika tárgy keretében, építve a megszerzett adatmodellezési ismeretre, egy választott személyközlekedési mód/szolgáltatás információs rendszerét tervezik meg a hallgatók. Célunk, hogy az elméleti rendszertervezési ismereteket a gyakorlatban is tudják alkalmazni. A rendszertervezési alapelvek mellett, innovatív megoldásokkal (pl.: big data, mesterséges intelligencia) is megismerkednek a hallgatók. A féléves házi feladat egy személyközlekedési információs rendszer bemutatására, értékelésére, összehasonlítására és továbbfejlesztési javaslatok kidolgozására, ezekhez rendszerkoncepció és rendszerterv készítésére terjed ki. Építve az alapképzésen szerzett tudásra a választott információs rendszer (vázszerkezeti, működési modell) és az adatbázis-szerkezet megtervezése (adatmodellezés) is a feladat része.

A főbb vázlatpontok a következők:
– felépítés (alrendszerek, gépi és humán komponensek, azok kapcsolatai, a kapcsolatok mögötti információáramlás jellemzői),
– funkciók, működés (folyamatábrák – részfolyamatok logikai és időbeli függései),
– kezelt adatok forrása, hitelessége, aktualitása,
– külső információs kapcsolatok (interoperabilitás),
– szervezeti követelmények (struktúra),
– üzemeltetési jellemzők,
– felhasználói felületek, megjelenítés,
– az információs szolgáltatás szintjei (pl. esemény + helyszíne, időpontja, időtartama + következménye + alternatív ajánlat),
– költségek (hardver- és szoftverfejlesztés, üzemeltetés – az információ értéke, haszna),
– adatbiztonsági kérdések.

A tématerület megismerése érdekében a hallgatók tudományos, nemzetközi irodalomkutatást is végeznek. Az eredményeket dokumentálják és a félév végén prezentáció formájában bemutatják.

Összefoglalás

A BME közlekedésmérnök hallgatói széleskörű elméleti és alapos gyakorlati tudásra tesznek szert közlekedési informatika témakörben. Az alapképzésben alkalmazott közlekedésinformatikai tudást sajátítanak el, megismerik a legfontosabb közlekedési információs rendszereket. A gyakorlatokon az elméleti oktatáshoz kapcsolódóan adatmodellt és adatbáziskezelő alkalmazást fejlesztenek egy-egy közlekedési témában. A mesterképzésben az információs rendszerek felépítését és működését leíró modelleket ismernek meg, mely tudást felhasználva a gyakorlati órákon egy információs rendszer koncepcionális tervét készítik el. A tananyag fejlesztése folyamatos, az innovatív megoldásokat (pl. elektromos és autonóm járművek üzemeltetése) beépítjük az oktatásba. A „iskolai jellegű” feladatokon keresztül szerzett tapasztalatokkal a hallgatók később eredményesen tudnak bekapcsolódni összetettebb, nagyobb léptékű, komplex rendszertervezési és -fejlesztési feladatokba is, ahol ezek az alapismeretek és készségek nélkülözhetetlenek.



SZAKÁCS BALÁZS *

Középiskolai tanulók biztonság-tudatos informatikai eszközhasználatának vizsgálata 1. rész

Összefoglalás: Célom naprakész felmérés készítése egy esztergomi gimnázium nappali tagozatos tanulóinak IKT eszközhasználati szokásairól, melynek segítségével tervezhetővé válik a biztonságtudatos eszközhasználat kialakítása a jövőben. A mindennapok részévé vált napjainkban az informatika, az eszközei, a használatuk; a hírekben naponta hallunk a kibertérben végrehajtott negatív tevékenységekről. A tanárok a diákokkal és egymással is a különböző szociális hálókon tartják a kapcsolatot, valamint Magyarországon is alkalmazásra került az európai általános adatvédelmi rendelet (GDPR). A diákok egész nap „online" vannak, mindent megosztanak, véleményeznek, ennek ellenére az ismereteik az internettechnológia valamit a biztonság területén felületes. A kutatás során választ kaphatunk arra, hogy a diákok ismereteit szükséges-e bővíteni, vagy tudatosan használják az eszközöket ismereteikkel összhangban.
Kulcsszavak: Informatikai biztonság, középiskola, tudatosság, kutatás.

Abstract: My goal with this research was to design and conduct an up-to-date cyber security awareness survey at one of Esztergom's high-school. The results of this survey will highlight the students everyday behavior regarding security and privacy related issues, and based on this outcomes we can tailor generation-specific education materials in the future. As IT became part of our everyday life, we hear cyber security related news (like data breaches, malware and hacker attacks) day-by-day. Students and teacher stay connected through various social platforms, and the European General Data Protection Regulation (GDPR) was approved in Hungary. These reasons inspired my to conduct my research. Students are "online" all day, they comment and share everything, but even so they have superficial knowledge about IT systems and the security-privacy related topics. I will answer to the question whether student need to broaden their knowledge or do they use their gadgets in accordance with their knowledge.
Keywords: IT Security, high school, awareness, privacy.

* *Dunaújvárosi Egyetem, Mérnöktanár levelező hallgató*
E-mail: leveldettinek@gmail.com

[1] Központi Statisztikai Hivatal

[2] KSH 2018 106. oldal

Bevezető

A tanulmányaim részeként került végrehajtásra egy empirikus kutatás, amely vizsgálja a mai középiskolai tanulók informatikai biztonságtudatosságát. A munkakörömből kifolyólag a közoktatásban a kötelező tanítási gyakorlat kivételével nincsenek tapasztalataim, így olyan témát választottam, amely megfelel az érdeklődési körömnek, meglátásom szerint kutatható, napjainkban figyelmet kap, mégsem került még gyakran elemzésre. Ezek alapján a biztonsági területet helyeztem a középpontba, így olyan területen hajtottam végre a feladatot, ami számomra ismert, és a későbbiekben a gimnáziumi oktatásom alatt, ahol IT-biztonságot tanítok 2 féléven keresztül, hasznosítani tudom. A téma választásánál azt az aranyszabályt követtem, hogy legyen kutatható, érdeklődjek a téma iránt, ne legyen számomra közömbös, és legyen haszna, ne csak a fióknak készüljön. Ezek figyelembevételével a kutatásmódszertan tanulmányozása mellett megfogalmazásra került, hogy lehetőleg a szakterületemmel kapcsolatban álljon (IT), a végrehajtásra megfelelő az iskola, ahol a gyakorlatomat végzem (Tatabányai Szakképzési Centrum Bottyán János Szakgimnázium, Esztergom). Ezek ismeretében a következő félévtől általam oktatásra kerülő tantárgy (IT-Biztonság) leszűkítette a lehetőségeket. Rövid tervezés után döntöttem el, hogy a biztonságtudatos IT-eszközhasználatot fogom kutatni. A mindennapokban két közoktatásban tanuló gyermekemmel kapcsolatban is tapasztalom a pedagógusok online kapcsolattartását, a Facebook erőltetett használatát, a felelőtlen fotók és egyéb információk megosztását. Az ismeretek hiánya miatt a „zárt csoport" mint misztikus, mindenki más számára láthatatlan tevékenységi tér használatát, és a diákok között is ennek a terjedését. A vírusként a csoportokon keresztülfutó új applikáció telepítési igényét, a telefonokon a rendelkezésre álló hely rohamos fogyását, valamint az influencerek, celebek, youtuberek görcsös like- és követővadászatát. A kibertérből gondolkodás nélkül elfogadott és átvett viselkedésminták utánzását. A szakirodalom kutatásakor nem találtam ezzel célirányosan foglalkozó kutatást, így munkám úttörőnek tekinthető.

Jogi háttér

A KSH [1] adatai szerint [2] a magyarországi otthonok 82% rendelkezik internetkapcsolattal (2017-es adat), viszont az azóta eltelt időben az internetelérés ára csökkent, így elterjedtek az internetkapcsolatot használó mobiltelefonok és alkalmazások. Emellett az in-

ternethasználat „online elérhetőség" a 16–24 éves korosztályban 94% volt. Ebből látható, hogy a mindennapjaik részét képezi az internet, a felhőszolgáltatások és a szociális hálók használata. Bár rendelkezik az ország Digitális Oktatási Stratégiával 2016 óta, és kutatják az informatikai lefedettséget, IKT [3] szokásokat, az iskolai eszközhasználat, a tudatos eszközhasználat nem került mérésre. Magyarország Kormánya a 1536/2016 (X.13.) Kormányhatározat a köznevelési, a szakképzési, a felsőoktatási és a felnőttképzési rendszer digitális átalakításáról és Magyarország Digitális Oktatási Stratégiájáról, valamint a 1139/2013 (III.21.) Kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról kijelölte az irányokat. Itt kerül, meghatározásra a biztonságos és megbízható kibertér, mint követelmény, említésre került a gyermekek veszélyeztetettsége, valamint a fiatalok nevelésének a pozitív minta alapú viselkedésformálása. A diákok ismeretei elenyészők az internettechnológiák területén, nem értik, hogy tevékenységük kárt okozhat másoknak és saját maguknak. Az Európai Parlament és a Tanács (EU) 2016/679 [4] rendelete (2016. április 27.) szabályozza egyebek mellett a személyes adatok védelmét és kezelését. Ezek együtt viszont csak a jogszabályi környezetet határozzák meg, a felhasználóknak és a szolgáltatóknak ezen keretek között kellene tevékenykedniük, amelyek beemelésre kerültek a magyar jogalkotásba. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénybe 2018. 07. 26-i módosítással. A következő szabályozás a 2019. évi XXXIV. törvény az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról, amely a még nem részletezett területeket próbálta meg lefedni, amely 2019. 04. 26-ától érvényes. Ezek alapján azt lehet megállapítani, hogy a jogszabályok az EU szabályaival harmonikusan a biztosítják jogi környezetet.

[3] Infokommunikációs technológia

[4] GDPR General Data Protection Regulation

Szakirodalmi háttér áttekintése

A szakirodalom áttekintése több egymástól független területre csoportosítható: ezek az internettechnológia (IT), tudatosság és biztonság, valamint a pedagógiai nevelés. Az informatikai biztonság meghatározásával kezdeném, habár a tudományos életben, ebben – mint sok egyéb másban – nincs egyetértés. A biztonság meghatározásakor viszont összefüggések, területek különülnek el egymástól, ezek az alkalmazkodás, a veszély tudatos felmérése, kezelése, elemzése, valamint a reagálás minden változásra. Az értelmező kéziszótár szerint a tudat a veszély tudata, míg a tudatos cselekvés olyan magatartás, amely a tudaton alapszik illetve világosan a tudatban van. Ez azt jelenti, hogy a személyek akkor képesek tudatosan cselekedni, ha ismerik az esetleges veszélyeket, valamint tudatában vannak cselekményük

súlyával, illetve a várható következményekkel. Tudományos körökben a tudat megfogalmazásánál Kihlstrom [5] megközelítése az egyik elfogadott, mely szerint „a tudat önmagunk és környezetünk folyamatos követése, valamint ezek folyamatos kontrollja, amely lehetőséget biztosít a viselkedéses és kognitív cselekedetek végrehajtására".

Az informatikai biztonság megfogalmazásához először az információ (adat) biztonságot szükséges definiálni. „*Az információbiztonság a biztonságtudomány részterülete, amely „az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb tulajdonságok, mint a hitelesség, a számon kérhetőség, a letagadhatatlanság és a megbízhatóság szintén ide tartozhatnak*". [6] Az informatikai biztonság ennek csak egy része, annak az állapotnak az elnevezése, amikor az elektronikus rendszeren kezelt adatokra és az elemeire vonatkoztatjuk. Alapvetően három fő területe van az IT-biztonságnak, ezek a hardver, szoftver és az emberi tevékenység. Ezek közötti különbség legkönnyebben úgy érthető meg, hogy az első két esetben a felhasználótól elkülönül a felelősség, amely a gyártó és fejlesztő, végső soron az üzemeltető között oszlik el. Az emberi tevékenység a legkockázatosabb szegmense a technológiának, mivel az igények és elvárások exponenciálisan növekednek az userek részéről, miközben a tudatlanság, az ismeretek hiánya következtében téves biztonságérzetbe ringatják magukat. Az elfogadott meghatározás szerint az informatikai rendszerek esetén biztonságként az adatbiztonsági követelményeknek történő megfelelést értjük, ezek a bizalmasság, sértetlenség, rendelkezésre állás. Az eddigiekből belátható, hogy a teljes biztonság nem elérhető, viszont megfelelő magatartással, az esetleges kockázatok figyelembe vételével, elemzésével, kezelésével valamint a maradvány kockázatok vállalásával egy megközelítőleg stabilnak tekinthető környezet alakítható ki. A felhasználó számára ezek azt jelentik, hogy a privát adataik nem kerülnek illetéktelen személyek kezébe, azokat más nem képes módosítani, valamint elérhetőek, amikor szükséges. Ezeknek a biztosításához viszont nem elégséges a szolgáltatói oldal, a kibertérben történő védelem, mivel egy rossz döntéssel az adatokat a felhasználó is megadhatja, bárki számára hozzáférhetővé teheti. Ennek veszélyeiről elméletileg tájékoztatnak a felhőszolgáltatások, szociális hálók, de a vizsgált korcsoport alapvetően nem olvassa el a tájékoztatókat, hanem a „Next – Next – Finish" klasszikus alkalmazásával, a gyors telepítést létesítik előnyben. Ebben a megközelítésben kibertérnek tekintve az elektromágneses spektrum használatával meghatározható dinamikusan változó tartományt, amely egymással kapcsolatban álló eszközök és hálózatok, valamint ezek működését biztosító infrastruktúrák összességét. Az oktatásokon, a szolgáltatások hozzáférés-kezelését is csodálkozva hallgatják a diákok, viszont a legújabb applikációkat is azonnal letöltik, ha megjelenik valakinél, majd keseregnek a kevés tárhely, a rendelkezésre álló kevés mobil adatforgalom lehetősége, az eszközök sebességének csök-

[5] John Federick Kihlstrom amerikai pszichológus

[6] http://infoter.eu/video/informacio-biztonsag_inteju_sik_zoltan_nandor

kenése, valamint a térerő miatt. Az adatok biztonságos hozzáférését háromféle azonosítás védheti a kibertérben, illetve a saját eszközökön, ezek a tudás (felhasználónév, jelszó), tulajdon (Mobil, PC), és tulajdonság (ujjlenyomat). Ezek közül legalább kettőt szükséges használni (kétlépcsős hitelesítés), amely a három típust jelenti.

Az informatikai rendszerek csoportosításánál napjainkban megjelent a PAM (Personal Area Network) amely a felhasználó IKT-eszközeinek gyűjtőfogalma, elvárás, hogy minden eszköz szinkronizáljon egymással, az adatok elérhetőek legyenek. Ennek a hálózati adatforgalmának vizsgálatától eltekintve, belátható, hogy az eszközök közül bármelyiknek a sérülékenysége az egész rendszert és így az azokon tárolt adatokat is veszélyezteti. A felhasználó kényelmi igényeit a biztonsággal ütköztetve a felhasználók általában a kényelem irányába hajlamosak dönteni. Ezért használják az eszközeiket rendszergazdaként, valamint az összes eszközön ugyanazzal a jelszóval (ami soha nem jár le, és személyük ismerete esetén megfejthető), bejelentkezni. Nem megértve azt a biztonsági kockázatot, hogy ilyenkor minden rendszer a rajta kezelt adat, alkalmazás hozzáférhetővé válik egy eszköz megszerzése által.

Fenyegetések

Az elmúlt egy évben a világon 92545453 spam volt jelentve, ami átlagosan 2,9, a maximális mennyiség 6,3 levélszemét másodpercenként. [7] A következő veszélyforrások a szoftveres vírusok: olyan programok, amelyek a megfertőzött program működésekor képesek önmagukat lemásolni, sokszorosítani. A mai modern káros szoftverek már módosítani is képesek magukat, így több változatban is képesek magukat terjeszteni, ez az önvédelmi mechanizmusuk része. A vírusok másik elterjedt csoportja a trójai programok, amelyek valamilyen szolgáltatást nyújtanak (vagy ígérnek), viszont tevékenységük a háttérben ettől eltérő (adatszerzés, módosítás, törlés). A zsaroló vírusok az utóbbi évtized egyik elterjedt pénzszerzési módszer a hackerek körében. Az IKT-eszközökön tárolt állományokat algoritmussal kódolják, majd törlik is, illetve megakadályozzák a hozzáférést az adott eszközhöz vagy rendszerhez, hacsak nem fizet a fertőzött rendszer tulajdonosa. Az ilyen támadások számát nehéz becsülni, mivel a magánszemélyek a berendezéseket újra telepítik, és nem jelentik be. Az állami cégek esetén nem ilyen egyszerű az incidens kezelése, ha képesek, akkor az adatokat helyreállítják, ha nem fizetnek, vagy elveszítenek minden érintett adatot. A holland kiberbiztonsági központ jelentése szerint [8] legalább 1800 vállalat szenvedett zsarolóvírus-támadást, közöttük legalább egy kritikus infrastruktúra.

[7] https://www.spamcop.net/spamgraph.shtml?spamstats letöltve 2019. 11. 27. 13:07.

[8] https://www.bleepingcomputer.com/news/security/dutch-govt-warns-of-3-ransomware-infecting-1-800-businesses/

[9] Intrusion Detectoin System – Intrusion Prevention System

[10] www.fbi.gov/investigate/cyber

Az informatikai biztonsági rendszerek is fejlődéseken mennek keresztül, de összetettségük és a felhasználók nagy száma miatt a tűzfalak használata helyett már a komplex IDS–IPS [9] rendszereket részesítik előnyben, a kollektív védelmet és a felhasználók tudatosságának képzését. Az IKT-eszközökhöz a gyártók biztosítanak operációs rendszert, PC esetén külön szükséges beszerezni. A jogtiszta szoftverek frissítését meghatározott ideig kifutási rendszerben biztosítja a szoftvergyártó. A Windows®-rendszer 2019. 07. 01. óta 34 frissítést adott ki a saját tulajdonú asztali berendezésemre vonatkozóan, 18 minőségi, 4 illesztőprogram, 6 definíció és 6 egyéb frissítést (2019. 12. 04-ei állapot). A frissítések kezelésénél ezért fontos az azonnali végrehajtás, mivel ezekkel foltozzák be a felfedésre került sérülékenységeket is. Az operációs rendszereken kívül a felhasználásra kerülő szoftverek is frissítésre kerülnek, az Android IOS-t futtató eszközök, a biztonságos forrásból származó applikációkat megfigyelésem szerint havonta frissíti. A felmérés végrehajtásakor a napjainkban legelterjedtebb veszélyeket mértem fel, amelyek a vírusok, trójai programok, zsarolóvírusok, kéretlen levél (spam), álhírek (fake news, hoax), adathalászat (phising), a manipuláció (social engineering). A két új típusú online jelenség, amely a fiatalok körében terjed, a megfélemlítés (bullying) valamint a kiközösítés. Az ilyen cselekményeket végrehajtó személyek nincsenek sokszor a tudatában, hogy bűncselekményt követnek el a tevékenységükkel. Sokan élnek abban a tévhitben, hogy a kibertérben végrehajtott tevékenységük rejtve maradhat, annak ellenére, hogy a szolgáltató naplóz mindent. Ezt a hozzáállást csak a technológia ismeretének hiánya magyarázza meg. A kutatásom tervezésekor szembesültem azzal, hogy a felhasználók nem értik, hogy az internetre egyszer feltöltött anyag örökre ott marad.

Az FBI [10] jelenleg három elsődleges veszélyt határoz meg, ezek a „Going Dark", azon tevékenységek gyűjtőfogalma, amikor a jogrendszerekkel szembenálló csoportok olyan módszereket használnak, amivel rejtve maradhat a tevékenységük. A következő, ami országunkban nem jellemző, az „Identity Theft", amikor valakinek az adataival visszaélnek, ellopják a személyi adatait, jogtalan haszonszerzés vagy más bűncselekmény elkövetésének érdekében. A harmadik csoport az „Online Predators" azaz internetes ragadozók, akik az áldozataikat keresik az online térben. Ezek a tevékenységek azonban nem számottevők hazánkban.

A kibervédelem az IT-biztonság napjainkban használt gyűjtőfogalma, a védelmi megoldások fejlődésének kiterjesztése a fizikai eszközök és szoftvereken kívül magában foglalja a kockázatok elemzését, a felhasználók és üzemeltetők elvárt viselkedését is. Ennek fontos részét képezi az ismétlődő oktatás, a szabályok és szabályza-

tok betartásának és betartatásának ellenőrzése, a hiányosságok felfedése, és arányos szankciók alkalmazása. Főbb részei a hálózatbiztonság (statikus, wireless), hálózati behatolásvédelem, alkalmazásbiztonság, alkalmazásbehatolás-teszt, kockázatelemzés. Magyarországon a 2012-es Global Cybersecurity Index & Cyberwellnes Profiles [11] felmérése szerint a lakosságnak 72,64% a használ internetet, a világ országai közül rangsorban pedig a 6. (megosztva), 0,676-os mutatószámmal. A szakemberek felismerték annak fontosságát, hogy a gyermekek informatikai eszközhasználati ismereteit nem szabad csak a véletlenre bízni, mivel az ismeretek fejlesztése társadalmi feladat, az egész nemzet biztonságtudatos magatartását befolyásolja a fejlettsége. Az alapok elsajátításában kiemelkedő szerepe van a családoknak, a szülőknek, valamint az oktatási intézményeknek. A gyerekeknek az informatikai eszközökkel való első találkozástól fontos a biztonságtudatos szocializáció. Az első találkozásokat pedig követi az élethosszan tartó tanulás.

Az általam vizsgált oktatási intézménybe a diákok az IKT-eszközöket a termekben tanári felügyelet mellett használhatják, a tevékenységek rögzítésre kerülnek. A berendezéseken felhasználói fiókokkal rendelkeznek, amelyeken a tárolt adatok biztonsági mentésre kerülnek. A *logók* [12] visszaellenőrzése csak incidens esetén történik meg. Minden informatikai teremben kifüggesztésre kerülnek a felhasználással kapcsolatos szabályok. Az iskolában a diákok által elérhető vezetéknélküli hálózat internetkapcsolat nincs üzemeltetve.

Magyarországon egyre jobban terjed a BYOD [13], amely az iskolákban is megjelenik, az esetenként elavult eszközök használata helyett elnézik vagy engedélyezik a saját eszközök bevitelét és az azokon történő feladatvégrehajtást. Ezzel viszont adat- és hálózatkezelési problémák merülnek fel. Az általam vizsgált intézményben a saját eszközök használata nem tiltott, viszont az iskola belső hálózatához és erőforrásaihoz nem kapcsolódhat közvetlenül. Ez azt jelenti, hogy az internetkapcsolatot igénylő esetekben a tanulónak az adatkapcsolatot saját költségen szükséges biztosítani.

A pedagógia összetett fogalom, elméleti és gyakorlati területeket is magába foglalva, az eredményességét a gyakorlatban történt alkalmazása határozza meg. Ez a körforgás, amely soha nem ér véget, önmagát fejleszti, módosítja. A pedagógia az informatika rohamos fejlődésével folyamatosan fejlődik, átalakul, valamint fejlődése felgyorsul. A tanárok, pedagógusok a rendszerben betöltött szerepüktől, általuk tanított tárgyaktól függetlenül nem tudják megkerülni, áthidalni a változásokat. Az IKT-eszközök elterjedésével az oktatás szerves részévé vált az informatika és ezzel az

[11] www.itu.int/dms_pub/opb/str/D-STR-SECU-2015-PDF-E.pdf

[12] Időbélyegzővel ellátott digitális naplóbejegyzés

[13] Bring Your Own Device

[14] Nemzeti Alaptanterv

informatikai eszközök használata, birtoklása, mégsem kapja meg a szerepe szerinti figyelmet a nevelésben. A közoktatás feladata az értékek közvetítése, a normák meghatározása. Ezekhez felhasználásra kerülnek a múlt elemzése, a jelen pontos ismerete és rögzítése, valamint egy jövőkép, aminek alapján felkészítésre kerülnek a diákok. A pedagógus felelőssége, hogy ezeknek a feladatoknak a legjobb tudása szerint eleget tegyen, a jövő nemzedékét a lehető legjobban felkészítve engedje ki a nagybetűs ÉLETBE. Ebben azonban partnerként kellene megjelennie a társadalomnak, a diákoknak és a tanároknak. A jövő pontosan nem meghatározható, de törekedni szükséges a lehető legszélesebb talapzat kialakítására, ahol a tanulók biztosan támaszkodhatnak majd a későbbiekben. Ebben kereteket szolgáltat a NAT [14], amely a helyi tanmeneteket meghatározza. A pedagógus szembesül azzal a ténnyel, hogy a technológia fejlődése miatt az ismeretei elavulnak, az ismeretanyagok méretei exponenciálisan növekednek, aminek az elsajátításában a tanulók nem partnerek. Fontos feladat lett az ismeretek szelektálása, mivel a szükséges tudás átadására az iskolák alkalmatlanok. A szaktudás és a társadalmi normák, az alapműveltség megszerzése (ami sok vitát generál) nem lehet csak az oktatási intézmények feladata, a szülőknek fontos lenne ezekben is szerepet vállalni.

A nevelés szerteágazó feladat, magába foglalja az erkölcsi, testi, esztétikai, értelmi és politechnikai nevelést. Az erkölcsi nevelés a társadalmi normákat közvetíti, a megfelelő magatartásformákat közvetíti, az emberek közötti viszonyt, magatartást szabályozza. Itt nehézséget okoz, hogy az írott és az íratlan szabályok közötti eligazodás, amit az iskolák oldanak fel, a lehetőségeikhez mérten. Az erkölcsi nevelés a magatartásformálást jelenti, aminek a következtében kialakul a jellem. Itt jelenik meg annak fontossága, hogy a sorkatonai szolgálat idejének lecsökkentése, majd szüneteltetése következtében a szabálykövetést, a feladatok végrehajtásának pontosságát megkövetelő időszak hiányzik azok életéből, akik most szülőként a gyermekeik nevelését az iskolákra bízzák. Az esztétikai nevelés a környezet és a mindennapok eseményeinek a megismertetését jelenti esztétikai eszközök segítségével. Fejleszti a befogadó és ítélő képességet valamint az aktív cselekvő alkotótevékenységet.

A belső tartalom szorosan kapcsolódik a külső megjelenéshez, ennek megfigyelhető megjelenése a hitelesség. A testi nevelés, napjainkban a fiatalok mozgásszegény életvitele, az egészségtelen táplálkozás és a káros szenvedélyek (dohányzás, tudatmódosító szerek) megjelenése miatt fontos. Az értelmi nevelés folyamatában korszerű ismeretekkel a világképet bővíthetjük, valamint azokat az egyéni képességeket (megfigyelés, emlékezet, képzelet, figyelem és problémamegoldás), amelyek nélkül az oktatásból kikerülő egyén képtelen lenne megoldani összetett feladatokat.

A politechnikai nevelés az eddigiek közül a legkevésbé költséghatékony, mivel az iskolát elkezdő személy (6–7 éves), számára az érettségi vizsga megszerzéséig (18–19 éves korig) folyton fejlődő eszközöket, műszaki megoldásokat kellene átadni. Ez lehetetlen, így a tevékenység a sokirányú műszaki alapok elsajátítására, a környezet megfigyelésének hasznosítására egy általános műszaki szemléletmód kialakítására fókuszál.

A kutatásról

A kutatás, amelyet végrehajtottam a tanulmányaim alatt, egy empirikus (alkalmazott kutatás), amelynek segítségével felmérésre kerülhet a vizsgált terület, és adatokat szolgáltathat a középiskolai gyakorlatom végrehajtásához az IT-biztonság oktatásához. Célom olyan ismeretek megszerzése, amelyek segítségével a valóság megismerhetővé válik, és ismereteket szerezhetek a jövőbeni pedagógiai tevékenységemhez.

A kutatás helyszíne

Magyarország területén Komárom–Esztergom megye, Esztergom város Tatabányai Szakképzési Centrum Bottyán János Szakgimnáziumban nappali tagozatos középiskolás személyek online kérdőívvel történő véletlenszerű kérdezése minimum 50 kérdőívvel.

A kutatás időtartama

A kutatás időtartama a rendelkezésre álló időkeret figyelembevételével 2019. 10 . 11–2019. 12. 16.

Az iskola bemutatása

A török uralom alól történő felszabadulás után 1683-ban Széchényi György esztergomi érsek alapítványa lehetőséget biztosított egy jezsuita gimnázium alapítására. Az első két osztály 1696-ban kezdte el a tanulmányokat a harmadik osztály elindítására 33 évet vártak. Az iskolát érintették a vallási és politikai alapú átszervezések, melyek néha bővítést, néha teljes átszervezést hoztak. Mária Terézia rendelete után 1775-től már három grammatikai egy retorikai és egy poétikai osztályt vittek. Az iskola jelenlegi helyére

[15] Forrás: www.bottyan.eu

1778-ban költözött. A szerzeteseket felváltották civil tanárok, 1786–1802 között, majd később a szerzetesek az oktatás színvonalát növelve fejlesztették az épületkomplexumot. Az újabb átszervezés 1849-ben leminősítette algimnáziummá, majd 1852-ben főgimnáziumi minősítést szerzett. 1853-ban a városi tanács a Szent Imre Gimnázium alapítását határozta el, amelynek ettől kezdve a Bottyánnal szorosan összefonódott a története, mivel annak jogutódjaként folytatta a tevékenységét.. Ezután az iskola fejlődése folyamatos volt az I. világháborúig, ami azonban a tanárok és diákok közül is több életet követelt. A második világégés alatt az épület több találatot kapott, majd 1944–1945-ig a tanítás szünetelt. Az iskola átköltöztetésre került a tanítóképzőbe. 1948.ban államosították, majd elköltöztették Vízivárosba ahol folyamatosan folyt az oktatás 2007-ig. A gimnázium 1972- től csak szakképzéssel foglalkozott I. István Ipari Szakközépiskola néven, 1975-től híradástechnikai képzés váltotta a gépgyártás-technológiai képzést. Technikusképzés 1985 óta folyamatos. A gimnáziumi képzés 1988-ban újra indult, és azóta is folyamatos. Az iskola 2007-ben diszlokált három évre Esztergom kertvárosba, majd 2010. 07. 01-én az eredeti helyére költözhetett, ahol 2013-tól 2015-ig a Klebelsberg Iskolafenntartó Központ fenntartásával működött.

Átszervezés után 2015. július 1-jétől a Tatabányai Szakképzési Centrumhoz került, ahol a 14 tagintézmény egyike lett, ahol az Emberi Erőforrások Minisztériuma majd a Nemzetgazdasági Minisztérium alárendelje lett. Szakmai irányítását pedig a Nemzeti Szakképzési és Felnőttképzési Hivatal vette át. Az iskola pedig 2017. szeptember 1-jétől új/régi nevet vett fel, így TSZC Bottyán János Szakgimnázium lett. [15]

Kutatási módszerek

A téma összetettsége miatt interdiszciplináris megközelítést választottam, mivel vizsgálni szükséges jog, informatika, pedagógia és pszichológia szemszögéből is. A szakirodalom vizsgálatakor törekedtem a hatályos jogszabályok áttekintésére, a kutatásban érintett kérdések megfogalmazásakor a közérthetőségre, tömörségre. Az összegyűjtött adatok elemzése statisztikai módszerekkel történt. A dokumentum-elemzéseket a saját témámhoz kapcsolódóan végeztem, azzal a céllal, hogy felmérjem a vizsgált tanulók IKT-eszközhasználatának szokásait, és így alapot szolgáltassak a jövőbeni oktatáshoz és kutatásokhoz. Kérdőívet készítettem, amelyet kitöltettem a vizsgált objektumban az alapsokaság részét képező entitásokkal.

Választott mérőeszköz

A felmérést a szakirodalom áttekintése után kérdőíven történő felmérés segítségével hajtottam végre 2019. 11. 04 00:00-tól 2019. 11. 29 00:00-ig. A tesztcsoport válaszainak kiértékelése után a kérdések számát csökkentettem 48-ról 25-re. A kérdőívek további kitöltése az online térben történt, önkéntesen, esztergomi középiskolás diákok körében.

Alkalmazott mintavételi eljárás

A kutatásomban alkalmazott mintavételi eljárás az egyszerű véletlen mintavételezés volt, mivel az alapsokaság homogén, véges elemszámú volt, a mintát visszatétel nélkül választottam (mindenki csak egyszer töltheti ki), elemenként egyenlő valószínűséggel. Mivel a teljes alapsokaság (435 fő) ismert így minden a felmérésben részt vevő személynek 1/435 esélye volt bekerülni a mintába. Mivel nem történt kényszerítés, az önkéntesség miatt a nemek és évfolyamok aránya nem reprezentatív a mintában, ezért az arányos elosztás nem biztosított. Ezeket a hiányosságokat későbbi kutatásaimban korrigálni tudom, a Neyman-féle optimális eloszlás segítségével, vagy a mintavételezés módosításával. Meglátásom szerint a 10% megfelelő arány, ha az elemek rétegeiből ezt prezentálni tudom. Viszont ennél a kutatásnál a rendelkezésre álló szűk időkeret miatt az előkészítés nem volt megfelelő ezek végrehajtásához.

Mintaösszetétel

A felmérésben érintett esztergomi középiskolás diákok, Előkészítőtől–Tizennegyedik évfolyamig minden csoport biztosított adatot, viszont az Előkészítő és a 14. évfolyam felülreprezentált, míg az érettségiző és 5. évfolyam hallgatói passzívak voltak. A nemi összetétel sem lett reprezentatív, mivel a lányok aránya nem közel azonos a fiúkéval, valamint a negyedikesek közül csak lányok válaszoltak a kérdőív kérdéseire.

Kérdések típusai

A kérdéseknél törekedtem a direkt kérdésekre, nem alkalmaztam a határidő miatt nyitott kérdéseket, hogy az elemzéseknél ne legyen kevés az időkeret. A zárt kérdések megoszlása típusuk szerint a következők: Alternatív kérdések: 1.1; 1.3; 2.1; 2.3; 3.1; 3.3; 3.5; 4.1; 4.2; 4.3; 4.4; 5.4; 5.7;

Feleletválasztást igénylő kérdések: 1.2; 1.4; 3.2; 4.5; 5.1; 5.2; 5.3;
Félig zárt kérdések: 2.2; 3.4; 4.6; 5.5;
Intenzitáskérdés (grafikus skála): 5.6.
A hipotézisekre a következő kérdések vonatkoznak:

1. A mai gimnazisták biztonságtudatosan használják informatikai eszközeiket. [3.1; 3.2; 3.3; 3.4; 4.1; 4.2; 4.3; 4.4; 4.5; 4.6; 5.1; 5.2; 5.3; 5.6]
2. A gimnáziumi diákok között nemek szerint vizsgálva az IKT biztonságtudatos használatban nincs releváns eltérés. [1.1-5.7]
3. A középiskolában az általam vizsgált csoportok az informatikai adataik biztonságáról gondoskodnak. [5.4; 5.5]
4. A felmérésre kerülő középiskolai tanulók átlagosan naponta legalább 4 órát online vannak. [1.4; 2.2; 3.5; 5.1; 5.7]

A próbakérdezés tapasztalatai

A végrehajtott próba-lekérdezés után a kérdőívből kikerültek az idegen szavak, az előkészítő osztályok számára is érthető kifejezések kerültek bele. A kezdeti kérdőív 48 kérdést tartalmazott, viszont a kitöltésnél a szövegek értelmezése, a kifejezések megértése is problémát okozott. A választási lehetőségeket lecsökkentettem, mivel a kérdőív kitöltésével kapcsolatos beszélgetésen kiderült, nem ismerik a kifejezéseket. A kérdésekben más változtatás nem történt, a mérés 5 fő véletlenül kiválasztott személlyel került végrehajtásra, anonim módon hagyományos papíralapú kérdéssorral. A kiértékelés során szigorítottam az online kérdéssort, a kérdések száma lecsökkent 25-re, valamint a „Nem tudom" válaszlehetőség mellett a kötelező kitölteni változtatás került az online kérdőívbe. A kitöltésre az egyéneknek megközelítőleg 6 perc volt szükséges, ezért a módosítások hatására megítélésem szerint 5 perc elegendő lesz. A kérdések csoportosítása véglegesítve lett, az 5 fő kérdéscsoportban a kérdőíven, valamint rögzítve lett az online kérdőív.

Alkalmazott módszerek

Az empirikus kutatásom kvantitatív, mennyiségi, szisztematikus adatgyűjtés anonim online kérdőívvel, randomizált (egyszerű véletlen) mintavételezéssel. Azért választottam ezt a módszert, mivel megbízhatósága magas, és elhanyagolható a kutatás szempontjából az eredmények torzulása, és nem célom a zárt kérdőívvel nem megszerezhető eredmények gyűjtése. Az névtelenség biztosítása miatt az alanyokról a nem és

az évfolyam kerül rögzítésre, semmilyen olyan adat nem, ami alapján visszakereshető vagy beazonosítható lehet. Mivel a kérdőív nem tartalmaz személyes adatokat, így az érvényben lévő adatkezelési szabályozásoknak megfelel, és nem szükséges az egyéneket, valamint hozzájárulásukat rögzíteni. Az alapsokaság meghatározásához a nyíltan elérhető adatokat vettem alapul, amelyek segítségével meghatároztam a felmérésben elégséges létszámot. Összesen 395 fő [16], nappali tagozatos diák és 58 fő az érettségi utáni OKJ képzésen vesz részt a felmérés időszakában. A tanulók megoszlása évfolyamonként *(1. számú ábra)*:

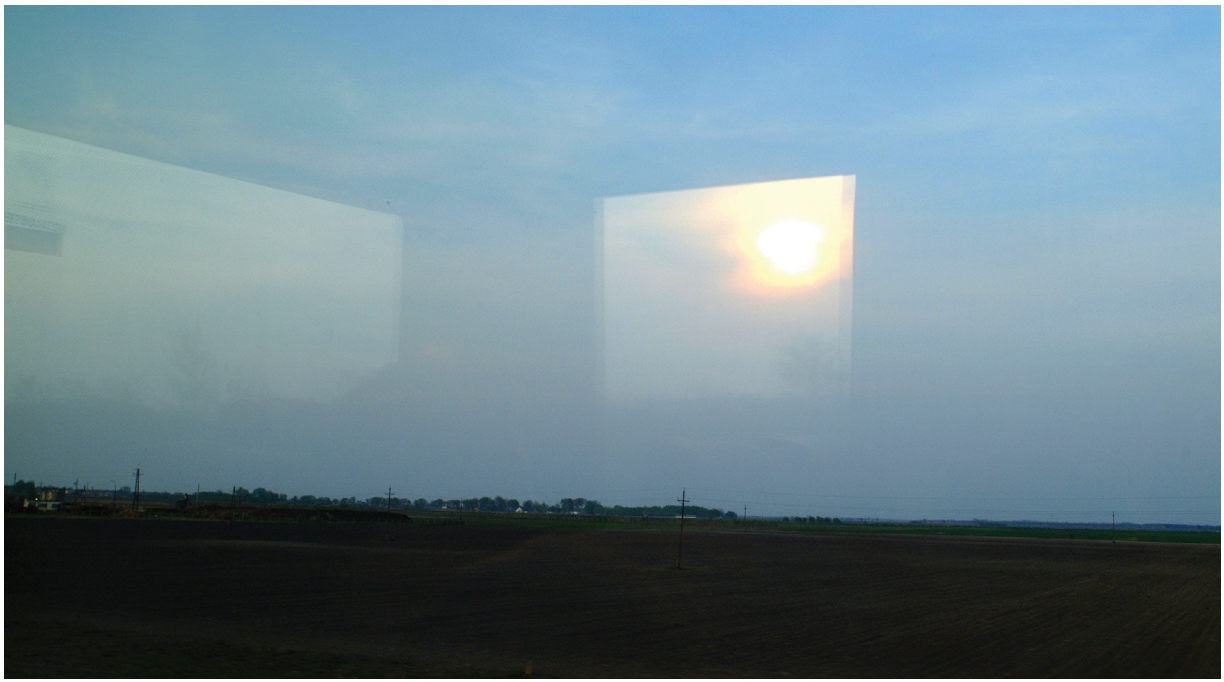
[16] www.bottyan.eu/k-kozzeteteli-lista/

1. ábra. Az alapsokaság és a kitöltések száma

Évfolyam	Létszám	10% fő	Kitöltötte			Kitöltötte %
			Összesen	fiú	lány	
Előkészítő	62	6	22	14	8	35,48
1.	92	9	39	31	8	42,39
2.	85	9	15	11	4	17,64
3.	82	8	10	5	5	12,19
4.	74	7	6	0	6	8,10
5.	45	5	4	1	3	8,88
6.	13	1	10	5	5	76,92
Összesen	453	45	106	67	39	

Ezek alapján 10% válaszadó megítélésem szerint megfelelő, ezért a kutatás eredményességének minimális értékeként 50 főt határoztam meg, ez a sokaság megközelítőleg minden 10. egyént jelentené. Az online kérdőív 250 főt képes mérni, a költségek optimalizálása miatt az e feletti kitöltések nem kerülnek rögzítésre. A kitöltést 106 fő hajtotta végre, így nem kerültek eldobásra kitöltött ívek. A beállításoknak köszönhetően, (kötelező válasz, minden eldöntendő kérdésnél, valamint legalább 1 válasz megadása kötelező), nem kerültek kitöltésre értékelhetetlen adatlapok.

Az írás 2. része a áprilisi számban következik.



KOVÁCS ISTVÁN BÉLA *

Riesz-terek típusairól röviden

Összefoglalás: A Riesz-terek egyes közgazdasági modellek alapját képező objektumok. Írásunkban megvizsgáljuk a jellemző tulajdonságaik által elkülöníthető tereket, egymással való kapcsolatukat.
Kulcsszavak: Rendezett vektortér, Riesz-tér, rendezési tulajdonságok.

Abstract: Riesz spaces are the underlying objects of certain models on economy. We inspect the different kinds of Riesz spaces distinguished by their characteristic properties in our talk. We outline their relationships also.
Keywords: Ordered vector space, Riesz space, Order properties.

* *Budapesti Gazdasági Egyetem, PSZK*
E-mail: kovacs.istvanbela @uni-bge.hu

Bevezetés

A múlt század '80-as éveire derült ki, hogy hogy a rendezett vektorterek, különösen a Riesz-terek közgazdasági modellek alapjául szolgálhatnak. Pontosabban, a topológiával ellátott Riesz-terekre hiteles gazdasági modelleket lehet építeni, melyek gyűjtőneve exchange economy [1].

Írásunkban most még a topológia hozzáadása nélkül ismerkedünk a Riesz-terek fajtáival, vizsgáljuk viszonyukat. Bizonyítást csak mutatóban közlünk a levezetések jellegének érzékeltetésére. Célunk annak bemutatása, hogy még topológia nélkül is mekkora a terület objektumainak gazdagsága.

Történet

Riesz Frigyes 1928-ban a Bolognai Nemzetközi Matematikai Konferencián tartott előadása indította el a róla elnevezett terek kutatását. Freudenthal és

[1] Aliprantis, Ch. D. – Burkinshaw, O. (20013): Locally solid Riesz spaces with applications to economics. *Mathematical survays and mongraphs.* 105. AMS.

Kantorovich rakták le az axiomatikus alapokat, és osztályozták a Riesz-tereket háló tulajdonságaik szerint. A következő évtizedekben a Nakano, Ogasawara, Yosida nevével jegyzett japán iskola, az oroszoknál Katorovich, Judin és Vulikh értek el fontos eredményeket. Luxemburg és Zaanen [2] az elméletet főleg a Banach-hálók keretében fejlesztették tovább. A hetvenes években jelentkezett az igény, hogy megvizsgálják a háló tulajdonságok kapcsolatát más lineáris topológiával ellátott Riesz-terekre is. Aliprantis és Burkinshaw, *Locally Solid Riesz Spaces with Applications to Economics* című monográfiájukat [1] ennek a célnak szentelték.
Írásunk felépítését erre a könyvre alapoztuk.

[1] Aliprantis, Ch. D. –Burkinshaw, O. (20013): Locally solid Riesz spaces with applications to economics. *Mathematical survays and mongraphs.* 105. AMS.

[2] Luxemburg, W. A. J. –Zaanen, A. C. (1963 –1964): Notes on Banach function spaces. *Nederl. Akad. Wetensch. Proc. Ser.* A, Notes I – XIII.

Fogalmak

Rendezett vektortér, Riesz-tér, netek, rendezés konvergencia

Egy valós vektortér E **rendezett vektortér**, ha adott rajta egy tranzitív, reflexív és antiszimmetrikus ≤ reláció, amely kompatibilis az algebrai struktúrával, azaz teljesíti a következő tulajdonságokat.

i) Ha $u,v \in E$ és $u \le v$, akkor $u + w \le v + w$ minden $w \in E$ mellett.

ii) Ha $u,v \in E$ és $u \le v$, akkor $\lambda u \le \lambda v$ minden $\lambda \ge 0$ számmal.

A vektortér null vektora 0, az $u \ge 0$ vektorok pozitív elemek. $E^+ = \{u \in E: u \ge 0\}$ a rendezett vektortér **pozitív kúpja**, röviden kúpja. A kúpok definiáló tulajdonságai

a) $E^+ + E^+ \subset E^+$,

b) $\lambda E^+ \subset E^+$ bármely $\lambda \ge 0$ számmal,

c) $E^+ \cap (-E^+) = \{0\}$.

Az i) ii) tulajdonságú rendezések és az a) b) c) tulajdonságú kúpok kölcsönösen egyértelműen meghatározzák egymást.

Definíció: Egy L rendezett vektorteret **Riesz-tér**nek nevezünk, ha L bármely véges, nemüres részhalmazának létezik szuprémuma L-ben.

Ismert, hogy ekvivalens definíciót kapunk, ha a véges, nemüres részhalmazok infimumának létezését követeljük meg. A szokásos jelöléssel $u \vee v = \sup\{u, v\}$ és $u \wedge v = \inf\{u, v\}$.

Az L Riesz-térben $u \in L$ fölbontható pozitív és negatív részének különbségére: $u = u^+ - u^-$, ahol $u^+ = u \vee 0$ és $u^- = (-u) \vee 0$. u abszolútértéke pedig $|u| = u^+ + u^-$ sok más érdekes tulajdonság mellett kielégíti a háromszög egyenlőtlenséget.

Harmadik megfogalmazásban, egy L rendezett vektortér Riesz-tér pontosan akkor, ha bármely $u \in L$ elemhez létezik u^+.

Egy Riesz-tér u, v elemeit **merőlegesek**nek (vagy diszjunktaknak) nevezzük, ha $|u| \wedge |v| = 0$.
Jelölése $u \perp v$.

Az irányított halmaz, ha értelmezett rajta egy $\lhd$ bináris reláció, amely reflexív, tranzitív és a következő tulajdonságot is kielégíti. Bármely $\alpha, \beta \in A$ párhoz létezik $\gamma \in A$, hogy $\alpha \lhd \gamma$ és $\beta \lhd \gamma$. Egy X halmazon értelmezett net egy leképezés $u : A \to X$, ahol A irányított halmaz.

A net szokásos jelölése $\{u_\alpha\}_{\alpha \in A}$, vagy csak $\{u_\alpha\}$. Egy $\{u_\alpha\}$ net növekvő, ha bármely $\alpha \lhd \beta$ indexpárra $u_\alpha \le u_\beta$. Jelölése $u_\alpha \uparrow$. Megfelelően definiáljuk a csökkenő neteket. Ha $\{u_\alpha\}$ növekvő net elemeinek létezik szuprémuma u, azt $u_\alpha \uparrow u$ jelöli, míg $u_\alpha \downarrow v$ szerint a csökkenő net infimuma v.

Definíció: Az L Riesz-térben $\{u_\alpha\}_{\alpha \in A}$ net **rendezésben konvergál** $u \in L$ elemhez, ha létezik $\{v_\alpha\}_{\alpha \in A}$ net L-ben, mellyel $|u_\alpha - u| \le v_\alpha \downarrow 0$. Jelölése $u_\alpha \xrightarrow{o} u$, u pedig az $\{u_\alpha\}$ net rendezés határértéke.

Állítás: Riesz-térbeli netnek legfeljebb egyetlen határértéke lehet.
Bizonyítás: Tegyük föl, hogy $u_\alpha \xrightarrow{o} u$ és $u_\alpha \xrightarrow{o} v$. Definíció szerint léteznek L-ben $\{x_\alpha\}$ és $\{y_\alpha\}$ netek, hogy $|u_\alpha - u| \le x_\alpha \downarrow 0$ és $|u_\alpha - v| \le y_\alpha \downarrow 0$.
Ekkor a háromszögegyenlőtlenség miatt $|u - v| \le |u - u_\alpha| + |u_\alpha - v| \le x_\alpha + y_\alpha \downarrow 0$.
Így $0 \le |u - v| \le 0$ miatt $u = v$. Legyen S részhalmaza L Riesz-térnek. S zárt a rendezésre, ha tartalmazza netjeinek rendezés határértékét.

Ideálok, sávok, alterek

Legyen S részhalmaz L Riesz-térben. S **szolid**, ha bármely $u \in L$ és $v \in S$ vektorokra igaz, hogy ha $|u| \le |v|$, akkor $u \in S$. Bármely $A \subset L$ halmazhoz létezik a legkisebb A-t tartalmazó szolid halmaz, az A szolid burka: $Sol\ A = \{v \in L : \exists u \in A$, hogy $|v| \le |u|\}$.

Definíció: Egy Riesz-tér szolid lineáris altereit **ideál**oknak nevezzük. A rendezett zárt ideálok neve **sáv**.

Definíció: Egy L Riesz-tér K lineáris alterét **Riesz-altér**nek nevezzük, ha tetszőleges $u,v \in K$ elemeivel együtt K tartalmazza azok L-beli szuprémumát és infimumát is, azaz L háló műveleteire zárt.

Az L Riesz-tér K Riesz altere **rendezés sűrű** L-ben, ha bármely $0 < u \in L$ elemhez létezik $v \in K$ mellyel $0 < v \leq u$. K **szuper rendezés sűrű** L-ben ha bármely $0 < u \in L$ elemhez létezik v_n sorozat K-ban, hogy $0 \leq v_n \uparrow u$ L-ben.

Riesz-terek típusai

Archimédeszi tulajdonság és Dedekind-teljesség

Definíció: Az L Riesz-tér **Archimédeszi**, ha bármely u, v pozitív elemeire $n \cdot u \leq v$ minden n természetes számra csak $u = 0$ esetén teljesülhet.
Tétel: Az L Archimedeszi Riesz-tér K Riesz alterére ekvivalensek

(i) A K rendezés sűrű L-ben.

(ii) Bármely $u \in L^+$ vektorra érvényes $u = \sup\{v \in K : 0 < v \leq u\}$.

(iii) Bármely $u \in L^+$ elemhez létezik $\{v_\alpha\}$ net K-ban, hogy $0 \leq v_\alpha \uparrow u$.

Egy további fogalom bevezetéséhez szükséges definiálnunk a Riesz-homomorfizmus fogalmát.
Legyenek L, M Riesz-terek. $\pi : L \to M$ lineáris operátor **Riesz-homomorfizmus**, ha $\pi(u) \wedge \pi(v) = 0$ M-ben, valahányszor $u \wedge v = 0$ L-ben (π háló homomorfizmus).

Most már bevezethetünk újabb típusú Riesz-tereket.

Definíció: Az L Riesz-tér

(1) **Dedekind teljes**, ha felülről korlátos nemüres részhalmazainak létezik szuprémuma.
(2) **Dedekind σ-teljes**, ha felülről korlátos, nemüres, megszámlálható részhalmazainak létezik szuprémuma.

(3) **Majdnem Dedekind σ-teljes**, ha L Riesz-izomorf valamely Dedekind σ-teljes Riesz-tér szuper rendezés sűrű Riesz alterével.

Nyilván fennálnak az 1) → 2) → 3) implikációk. A Dedekind-teljesség újabb változatához még egy fogalomra van szükségünk.

Definíció: L Riesz-tér rendelkezik a **megszámlálható sup tulajdonság**gal, ha bármely szuprémummal rendelkező S részhalmazának van megszámlálható részhalmaza, amelynek szuprémuma az S szuprémuma. A megszámlálható sup tulajdonsággal rendelkező Dedekind teljes Riesz-tereket **szuper Dedekind teljes** Riesz-tereknek nevezzük.

Projekciós tulajdonságok

Legyen A az L Riesz-tér nemüres részhalmaza. Jelölje $A^d = \{u \in L : u \perp A\}$ az A részhalmaz merőleges (diszjunkt) komplementerét. Az A^d minden esetben sáv. Teljesül továbbá, hogy $A \cap A^d = \{0\}$, $A \subset A^{dd}$, illetve, hogy $A \subset B$ esetén $B^d \subset A^d$. Igaz továbbá a következő fontos állítás.

Tétel: Ha A ideál L Riesz-térben, akkor $A \oplus A^d$ rendezés sűrű L-ben.
Egy L Riesz-tér B sávja **projektív** sáv, ha $B \oplus B^d = L$. Bármely projektív sáv meghatároz egy sáv projekciót a következő természetes módon. Ha $u = u_1 + u_2$, ahol $u_1 \in B$, $u_2 \in B$, akkor $P_B(u) = u_1$. Egy L Riesz-tér u elemét projektív elemnek nevezzük, ha az általa generált sáv projektív.

Definíció: Azt mondjuk, hogy az L Riesz-tér

(i) projektív, ha minden sávja projektív,

(ii) principálisan projektív, ha az egy elem generálta sávjai projektívek,

(iii) rendelkezik elegendő projekcióval, ha bármely nemzéró sávja tartalmaz nemzéró projektív sávot.

[3] Aliprantis, Ch. D.–Langford, E. (1974): Almost σ-Dedekind complete Riesz spaces and the main inclusion theorem. *Proc. Amer. Math Soc.* 44. Pp. 421–426.

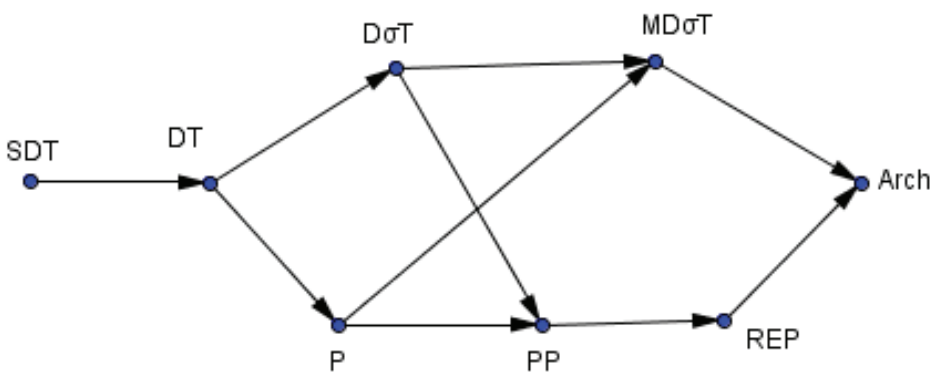
[4] Luxemburg W. A. J.–Zaanen, A. C. (1971): *Riesz Spaces I.* North Holland: Amsterdam.

[5] Quinn, J. (1975): Intermediate Riesz spaces. *Pacific J. Math.* 56. Pp. 225–263.

A Fő Tartalmazási Tétel

Ez a tétel foglalja össze a fönt felsorolt terek közötti összefüggéseket. Jelölje SDT a szuper Dedekind teljes, DT a Dedekind teljes, DσT a Dedekind σ-teljes tulajdonságot, míg MDσT a majdnem Dedekind σ-teljességet. Legyen továbbá P a projektív, PP a principálisan projektív, REP a rendelkezik elegendő projekcióval tulajdonság rövidítése. Arch jelenti az Archimédeszi tulajdonságot. Az alábbi ábrában a nyilak a tulajdonságok közötti implikációkat jelölik.

1. ábra.



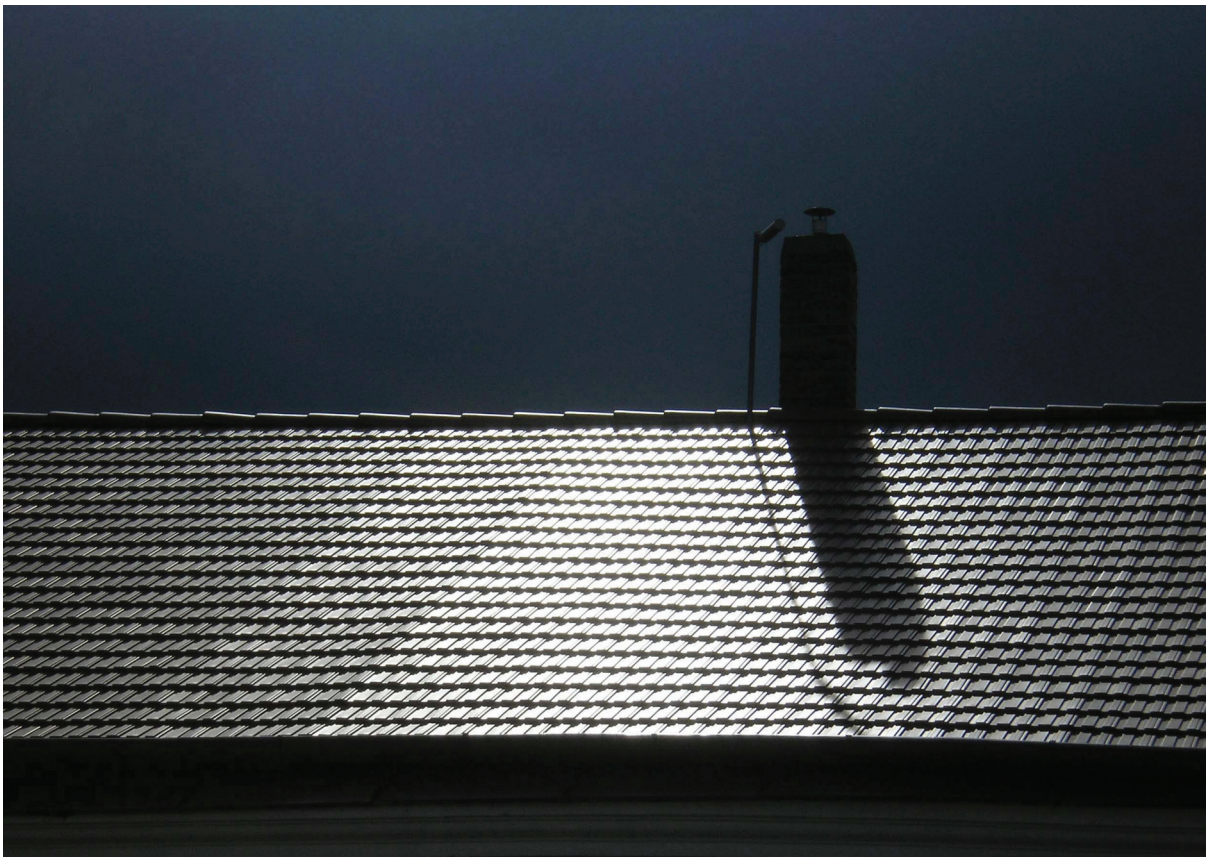
Az itt össze nem hasonlított tulajdonságú objektumok példákkal szétválaszthatók.

A majdnem Dedekind σ-teljesség kivételével a diagram következtetéseit Luxemburg és Zaanen adták meg [4]. A majdnem Dedekind σ-teljesség fogalmát Aliprantis és Langford [3], tőlük függetlenül Quinn [5] vezették be.

Példák

(1) Láttuk, hogy az osztályozásban szereplő terek mind Archimédeszi tulajdonságúak. A legismertebb nem Archimédeszi Riesz-tér $\mathbf{R}^2$ a lexikografikus rendezéssel: Lex, melyben $(x_1, y_1) \leq (x_2, y_2)$ ha $x_1 < x_2$, vagy ha $x_1 = x_2$ és $y_1 \leq y_2$. Lexben bármely két vektor összehasonlítható.
Pozitív kúpja $Lex^+ = \{(x,y) \in R^2 : 0 < x\} \cup \{(0,y) \in R^2 : y \geq 0\}$. Lex nem Archimédeszi, hiszen például $n\cdot(0,1) \leq (1,0)$ minden természetes számra, ám (0,1) mégsem a zéró vektor.
(2) Legyen L egy nem megszámlálható halmazon értelmezett valós függvények tere a pontonkénti rendezéssel. Az L Dedekind teljes Riesz-tér, ám nem szuper Dedekind teljes. Álljon S az egy elemű halmazok karakterisztikus függvényeiből. Ekkor sup S, a konstans 1 függvény nem állítható elő S megszámlálható részhalmazainak szuprémumaként.
(3) Legyen L a [0, 1] intervallumon értelmezett valós, Lebesgue mérhető függvények tere. Pontonkénti rendezéssel Riesz-tér. L Dedekind σ-teljes, mivel monoton növekvő korlátos sorozatok rendezésben is tartanak a szuprémumukhoz. Belátjuk, hogy L nem Dedekind teljes.
Ha L-ben $u_\alpha \xrightarrow{o} u$, azaz $|u_\alpha - u| \leq v_\alpha \downarrow 0$, akkor u_α pontonként tart u-hoz. Legyen E nem Lebesgue mérhető részhalmaza [0, 1]-nek, $\{\chi_\alpha\}$ pedig E véges részhalmazai karakterisztikus függvényeinek netje. Ekkor $\{\chi_\alpha\} \uparrow$ fölülről korlátos. Ha létezne szupremuma, ahhoz pontonként kellene tartania, azonban $\{\chi_\alpha\}$ pontonkénti határértéke $\chi_E \notin L$, úgyhogy L nem Dedekind teljes. Belátható továbbá, hogy L nem projektív Riesz-tér, de a Fő Tartalmazási Tétel szerint principálisan projektív.
(4) Legyen L = *c*, a konvergens valós sorozatok tere a pontonkénti rendezéssel. Az előadásunk anyagán túl mutató okok miatt L majdnem Dedekind σ-teljes, rendelkezik elegendő projekcióval, ám nem principálisan projektív.
(5) Kis módosítással legyen L a konstanssá váló valós sorozatok tere a pontonkénti rendezéssel.
Az L majdnem Dedekind σ-teljes, de nem Dedekind σ-teljes. Továbbá nem projektív, de principálisan projektív.
(6) Legyen L = C[0, 1] a pontonkénti rendezéssel. Az L nem rendelkezik elegendő projekcióval, de majdnem Dedekind σ-teljes.

A fönti példák nem választják szét a Fő Tartalmazási Tétel összes típusát, de jól mutatják a tulajdonságokat hordozó terek sokféleségét.



IMRE E.–BARRETO, D.–TALATA I.–

BAILLE, W.–RAHEMI, N.–GOUDARZY, M.–LŐRINCZ J.–SINGH, V. P.

Grading curves and internal stability
(A szemeloszlás és a belső stabilitás kapcsolata)

Abstract: The measured grading curve is an empirical distribution function, a step function. This is considered here as a discrete distribution with fixed statistical cells. In the grading entropy theory it is characterized by the relative entropy resulting in two sets of entropy coordinates. These first and second grading entropy coordinates classify well the grading curves and are statistically more soundly based in terms of information content than the approximate quantile type parameters used at present. In the theoretical and experimental work on the grading entropy coordinates, the physical content of the parameters are analysed. The results can be summarized as follows. The first entropy parameter seems to be a continuous internal stability measure. The second one allows the definition of a unique, mean grading curve with finite fractal grain size distribution for fixed value of the first parameter. The first parameter is related to internal structure, proven here by DEM tools. It is shown by Math tools that the probability of a stable state of the grading entropy theory is very low. The generally occurring stable states in the nature are originated from the degradation which is deterministic. The internal stability of the engineering structures can be characterized by grading entropy.
Keywords: Grading curve and grading entropy, internal stability, fractal, DEM.

Összefoglalás: A szemeloszlási görbe empirikus eloszlási függvény, lépcsős függvény, rögzített statisztikai cellákkal. Diszkrét eloszlásnak tekintve, alkalmazva rá a relatív entrópia definícióját, levezethető két ún. entrópia-koordináta. Ezek jól osztályozzák az osztályozási görbéket, és statisztikailag jobbak információtartalom szempontjából, mint a jelenleg alkalmazott közelítő kvantilisek, vagy kvantilis típusú paraméterek hányadosai. Az elméleti és kísérleti munka elemezi a paraméterek fizikai tartalmát. Az eredményeket a következőképpen lehet összefoglalni.

Óbudai Egyetem
E-mail: imre.emoke@kvk.uni-obuda.hu

Napier Egyetem, Edinburgh, U.K.
E-mail: d.barreto@napier.ac.uk

Ruhr Egyetem, Bochum, Germany
E-mail: wiebke.baille@ruhr-uni-bochum.de

BME
E-mail: lorincz.1947@gmail.com,

Texas A&M Edinburgh, College Station, USA
E-mail: vsingh@tamu.edu

Az első entrópia-paraméter egy folytonos belső stabilitásmértéknek tűnik. A második entrópia-paraméter lehetővé teszi egy átlagos szemeloszlási görbe meghatározását véges fraktál szemcseméret-eloszlással az első paraméter minden egyes értékére vonatkozóan. A mikromechanikai eredmények azt mutatják, hogy az első paraméter hogyan kapcsolódik a belső szerkezethez. Matematikai eszközökkel az az eredmény nyerhető, hogy a belső stabilitási szabály szerinti stabil állapot valószínűsége nagyon alacsony, a természetben a stabil állapot fordul mégis elő, ugyanis a talajok degradációja determinisztikus. A belső stabilitás a mérnöki földszerkezetek kulcsfontosságú paramétere.
Kulcsszavak: Szemcseeloszlás, belső stabilitás, fraktál, DEM.

Introduction

The grading curves of soils contain a large amount of data. This can render its use in the evaluation of soil properties awkward. Hence, rules based on a few nominated particle diameters have been developed (i.e. coefficients of uniformity and curvature, cu and cc, respectively). In more developed cases, some parametric functions are fitted to the grading curves or other approaches are used. However, these approaches are not valid for gap-graded grain size distributions. It is shown here that the two grading entropy coordinate pairs (base entropy and entropy increment), proposed by Lőrincz [1] may characterize the grading curves more effectively. They contain all measured data in terms of statistical means, and are related to internal stability.

Table 1. Fractions.

j [-]	1			23	24
Limits in d_o	1 to 2			2^{22} to 2^{23}	2^{23} to 2^{24}
S_{oj} [-]	1			23	24

[1] Lőrincz J. (1986): "Grading entropy of soils," *Doctoral Thesis, Technical Sciences*. TU of Budapest (in Hungarian).

Grading entropy

Space of grading curves

An abstract fraction system is defined. The diameter range for fraction j (j =1, 2...j, see *Table 1*) is:

$$2^{j}d_0 \geq d > 2^{j-1}d_0, \qquad (1)$$

where d_0 is the smallest diameter which may be equal to the height of the SiO_4 tetrahedron. The 2 base log of the diameter limits are integers, called abstract diameters. The relative frequencies of the fractions x_i *(i = 1, 2, ..N)* for each grading curve fulfil the following equation:

$$\sum_{i=1}^{N} x_i = 1, \qquad x_i \geq 0, \;\; N \geq 1. \qquad (2)$$

where the integer variable N – the number of the fractions between the finest and coarsest nonzero fractions– is used. The relative frequencies xi can be identified with the barycentre coordinates of the points of an *N*-1 dimensional, closed simplex (which is the *N*-1 dimensional analogy of the triangle or tetrahedron, the 2 and 3 dimensional instances), and the space of grading curves with *N* fractions can be identified with an *N*-1 dimensional, closed simplex.

Grading entropy parameters

jThe grading entropy S is a statistical entropy, modified for the unequal cells (fractions are doubled). It can be separated into the sum of two parts [1]:

$$S = S_0 + \Delta S \qquad (3)$$

where S_0 is base entropy and *S* is entropy increment. S_0 is a log "mean" of the diameter:

$$S_0 = \Sigma \; x_i S_{0i} = \Sigma \; x_i i \qquad (4)$$

[1] Lőrincz J. (1986): "Grading entropy of soils," *Doctoral Thesis, Technical Sciences*. TU of Budapest (in Hungarian).

where S_{0i} is the i-th fraction entropy *(Table 1)*. The entropy increment:

$$\Delta S = -\frac{1}{\ln 2}\sum_{x_i \neq 0} x_i \ln x_i \tag{5}$$

The relative base entropy *A* and normalized entropy increment *B*:

$$A := \frac{S_o - S_{o\min}}{S_{o\max} - S_{o\min}} = \frac{\sum_{i=1}^{N} x_i (S_{oi} - S_{o\min})}{N-1} = \frac{\sum_{i=1}^{N} x_i (i-1)}{N-1}, \quad B = \frac{\Delta S}{\ln N}. \tag{6}$$

where S_{0max} and S_{0min} are the entropies of the largest and the smallest fractions, respectively. Representing the space of the grading curves with N fractions by an N -1 dimensional, closed simplex, a secondary structure appear along to iso-surfaces of the normalised grading entropy parameters as follows. The grading entropy parameter A is a linear function, the *A* = constant condition defines parallel hyper-plane sections of the N-1 dimensional simplex, which are disjunct subspaces in the space of the grading curves *(Fig. 2)*. The grading entropy parameter *B* is a strictly concave function with a unique maximum for each *A* = constant value, which is a mean („optimal") point:

$$x_1 = \frac{1}{\sum_{j=1}^{N} a^{j-1}} = \frac{1-a}{1-a^N}, \quad x_j = x_1 a^{j-1} \tag{7}$$

where a is the root of the following equation:

$$y = \sum_{j=1}^{N} a^{j-1}[j-1-A(N-1)] = 0 \tag{8}$$

The optimal grading curves have fractal distribution, the fractal dimension is as follows [2, 3].

$$n = 3 - \frac{\log a}{\log 2} \tag{9}$$

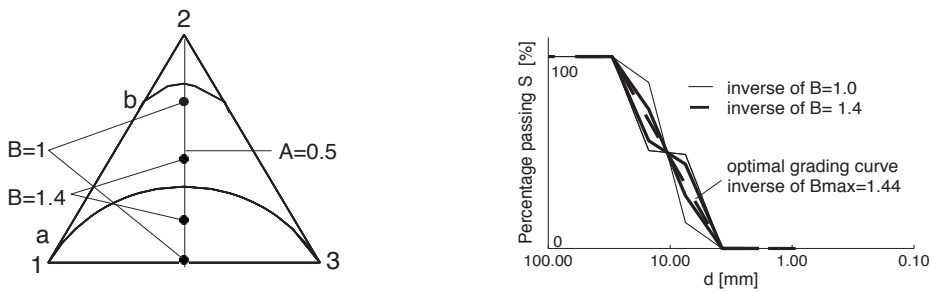
While a varies from 0 to 1 and 1 to ∞, A varies from 0 to 0.5 and from 0.5 to 1, n varies from ∞ to 3 and from 3 to -∞…respectively, at the two sides of the entropy diagram. Concerning the inverse image of a regular entropy diagram point [*A*,*B*] in

[2] Imre E.–Talata I. (2017): *"Some comments on fractal distribution,"* Proc. MAFIOK. Pp. 22–32.

[3] Einav, I. (2007): "Breakage mechanics – Part I." *Theory Journal of the Mech. and Physics of Solids.* 55: Pp. 1274–1297.

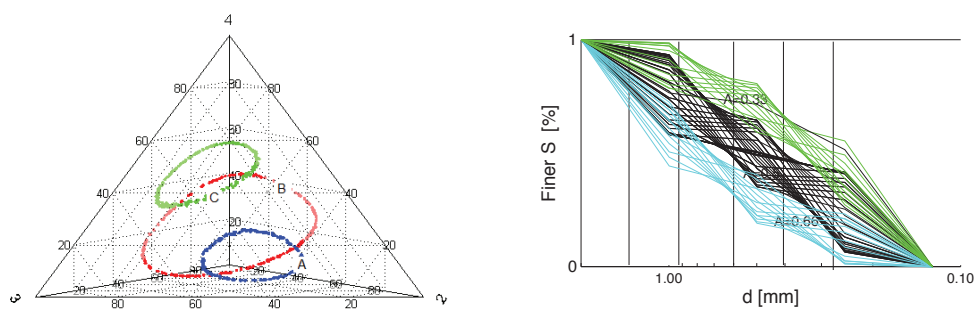
the simplex is an *N*-3 dimensional sphere, „centered" to the optimal point (of the *A* = const, *N*-2 dimensional hyperplane, *Figs. 1-2*).

Figure 1. N=3. (a) (b) The simplex points and the grading curves related to entropy parameters A=0.5 B=1. and A=0.5 B=1.4 which are topologically N-3=0 dimensional circles (point pairs and grading curve pairs).



(a) (b)

Figure 2. N=4. (a) (b) The simplex points and the grading curves related to entropy parameters A=0.66 B=1.2, and A=0.5 B=1.2, and A=0.3 B=1.2, which are N-3=1 dimensional topological circles (in the simplex and in the space of the grading curves).

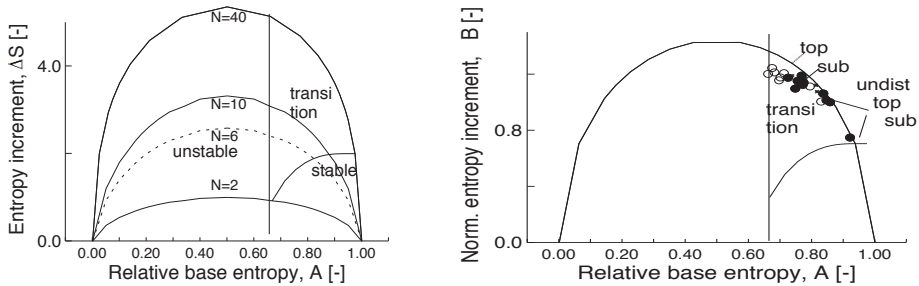


(b)

[1] Lőrincz J. (1986): "Grading entropy of soils," *Doctoral Thesis, Technical Sciences*. TU of Budapest (in Hungarian).

[10] Imre E. –Fityus S. (2018): *„The entropy as a measure of soil texture maturity and internal stability"* DECGE 2018. Pp. 639–644.

Figure 3. (a) Internal or grain structure stability criterion in the non-normalized diagram. (b) Internal or grain structure stability criterion in the N=17 related normalized diagram, with theindication of the degradation example of waste rock in open pit mine rehabilitation (thetopsoil samples are more degraded). [10]



(a) (b)

Grading entropy to describe internal stability

Four maps can be defined between a grading curve space (N-1 dimensional, open simplex) and the two dimensional space of the entropy coordinates: the non-normalized $\Delta\rightarrow [S_0,\Delta S]$; normalized $\Delta\rightarrow[A,B]$; partly normalized $\Delta\rightarrow [A,\Delta S]$ or $\Delta\rightarrow [S_0, B]$. Maps are continuous on the open simplex and can continuously be extended to the closed simplex for fixed N. The internal stability rule of the grading entropy theory [1] is defined by vertical flow tests on a partly normalized entropy diagram shown in *Fig. 3(a)*. There are three main zones.

For A < 2/3, the mixtures are internally unstable, for A = 2/3 and A > 2/3 the soils are internally stable, the structure gradually builds up for elongated grading curves. Suffosion may occur in each zone. The rule can be interpreted such that in Zone I (if A < 2/3) the coarse particles „float" in the matrix of the fines and become destabilized when the fines are removed by piping.

In the complementer zone (A = 2/3 and A < 2/3), the coarse particles form a skeleton, total erosion cannot occur. In Zone III, the structure of larger particles is assumingly inherently stable.

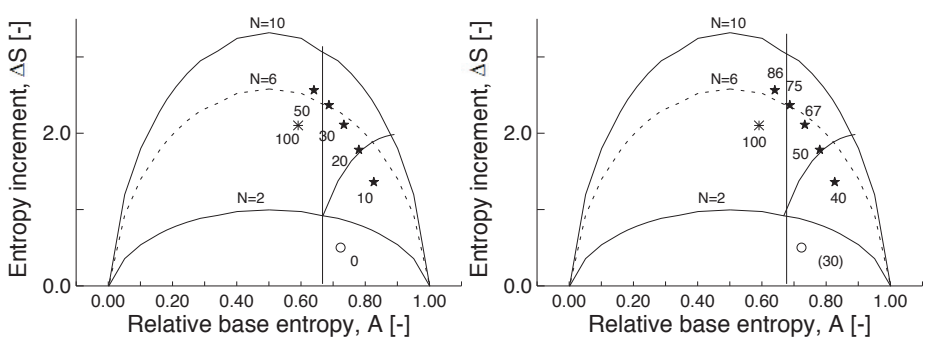
Table 2. The geometrical probability of the internally stable state in terms of the fraction.

N [-]	2	5	10	20	50
P(A>2/3)	3E-01	1E-01	4E-02	6E-03	2E-05

Table 3. Effect of grading entropy parameter A on the coordination number and critical friction angle - DEM and real experimental results.

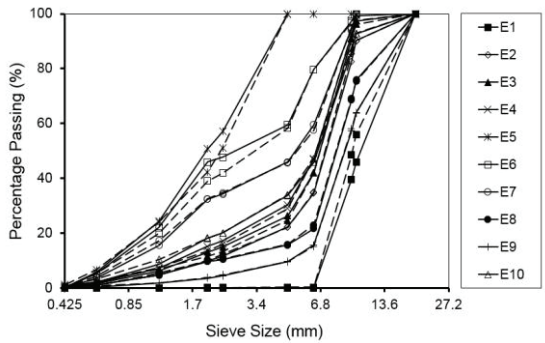
A [-]	Z [-]	Zm [-]	ϕ'_{crit} [°]	$\phi'_{crit,\,real}$ [°]
0.10	2.87	4.32	18.72	~33
0.33	2.34	4.41	18.43	~33
0.50	2.52	4.42	18.08	~34,5
0.66	2.83	4.47	17.85	~35.8
0.90	3.39	4.47	17.55	~36.5

Figure 4. Liquefaction susceptibility of Houstun sand - fine mixtures, varying fine content. Tests of Negar Rahemi in partly normalized diagram. (a) Gradings with various fine content percentages. (b) Probability of sample liquefaction at the previous points. (Note: bracket means that only limited liquefaction may occur.)

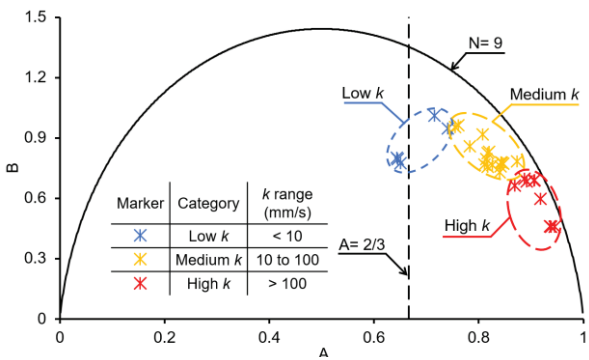


[11] Feng, S.–Vardanega, P. J.–Ibraim, E.–Widyatmoko, I. –Ojum, C. (2018): „Permeability assessment of some granular mixture” *Géotechnique.*

Figure 5. (a) Grading curve set out of three tested sets with varying fine content. (b) Permeability variation in normalised diagram [11].



(a)



(b)

Analysis of the internal stability rule

Internal stability and probability

The optimal or fractal grading curves have fractal dimension between - ∞ < n < ∞. The fractal soil is stable if $n < 2$, unstable at $A<2/3$ (n is varying in the function of N), transitional between these values. The natural soils [4, 5, 6] are generally fractal grading curves, the fractal dimension is between 2 and 3, being related to the stable-transitionally stable zones in terms of internal stability.

The geometrical probability expressed by the ratio of the volume of the simplex of the grading curves where A>2 /3 is met and the volume of the whole simplex tends to be zero (*Table 2,* [7]). This contradiction can be explained by the fact that the degradation process is deterministic but its discussion is beyond the scope of this paper (see eg., [12]).

Soil degradation in mine rehabilitation through degradation of waste rock over short time period is measured by studying the grading curve data ([10]). The grading curves are plotted in the transitional stability zone on the entropy diagram, with near fractal dimensions 2.5 to 2.8. A distinct difference for all sub and top samples is found: the topsoil is more degraded (*Fig 3b*).

Insights from DEM simulations

Preliminary 3D DEM simulations of spherical particles using periodic boundaries were performed. Four fraction sizes were used: 0.125-0.25 mm, 0.25-0.5 mm, 0.5-1 mm, and 1-2 mm (uniform distribution was assumed within the limits). 2-fraction soils (N=2) were tested with various A values under drained triaxial conditions until the critical state was achieved.

These DEM specimens were isotropically consolidated to 200 kPa and subsequently sheared with an inter-particle friction coefficient of 0.3. As a result their initial density is close to minimum and the overall (Z) and mechanical (Z_m) coordination numbers reflect this, as shown in *Table 3*.

[4] Miao, G.–Airey, D. (2013): „Breakage and ultimate states for a carbonate sand" *Geotechnique 63.* No. 14. Pp. 1221–1229.

[5] Palmer, A. C.–Sanderson, T. J. O. (1991): „Fractal crushing" *Proc R Soc London A Math Phys Sci 433*. 1889. 469–477.

[6] Coop, M. R.–Sorensen, K. K.–Bodas Freitas, K. K. –Georgoutsos, G. (2004): Particle breakage during shearing of a carbonate sand. *Geotechnique* 54(3): Pp. 157–163.

[7] Imre, E.–Barreto, D.–Talata, I.–Goudarzy, M.–Rahemi, N.–Baille, W. (2018): *Fractal and optimal gradings and their relationship to internal stability.* Atlanta. submitted.

[10] Imre E. –Fityus S. (2018): *„The entropy as a measure of soil texture maturity and internal stability"* DECGE 2018. Pp. 639–644.

[12] Lőrincz, J.–Imre, E.–Gálos, M.–Trang, Q. P.– Telekes, G.–Rajkai, K.–Fityus, I. (2005): Grading entropy variation due to soil crushing. *Int. Journ. of Geomechanics.* Vol 5:4. P. 31–320.

Note the coordination numbers represent the average number of contacts per particle for the specimen at the critical state. The mechanical coordination number is of particular relevance as it indicates the average number of contacts per particle, but in contrast to the overall coordination number, it only includes the particles which effectively transit stress (i.e. those that are part of strong force chains as normally reported in DEM studies).

Note that as *A* increases, Z_m also increases indicating that the number of particles effectively transmitting stress increases. Furthermore, as A increases, the difference between Z and Zm decreases. This implies that as A increases the number of „rattlers" (i.e. particles that are not part of the strong force chains) reduces. In other words, as A increases, the specimens become inherently more stable. In contrast, lower values of A indicate a higher likelihood of „rattlers" -or fines- that are potentially erodible. Hence, there is a clear link between stability, base entropy and mechanical coordination number.

Furthermore, the critical angle of shearing resistance seems to be dependent of A. This dependence relates to the inherent stability of the strong force chains, but its discussion is beyond the scope of this paper. It must be noted that the range of variation is nevertheless limited.

Examples on the effect of fines

A series of 60 conventional triaxial compression tests are conducted on Hostun sand –silt mixtures to investigate the effects of fines on the undrained monotonic response of sand [8]. *Fig. 4(a)* shows the mixtures with various fine content, Fig. 4(b) demonstrates that transitionally stable mixtures can increasingly be prone to liquefaction during static loading with increasing fine content if prectically all possible initial relative densities are considered [9] In a similar study, the boundary between the "fines-in-sand" and "sand-in-fines" micro-structure, the threshold fines content is found at around A=2/3 [9]. A correlation between the normalised grading entropy coordinates and the coefficient of permeability is presented [11]. Permeability depends on the voids. Some permeability zones are identified on the normalised entropy diagram on the basis of k values measured on 3 sets of grading curves. These zones follow rule that with decreasing A the fine content is increasing and the porosity is decreasing (*Fig. 5b*).

[8] Rahemi, N. (2017): „Evaluation of Liquefaction Behavior of Sandy Soils using Critical State Soil Mechanics and Instability Concept" *Ph D Thesis, Faculty of Civil Engineering, Ruhr-U Bochum.*

[9] Goudarzy M. (2015): „Micro and Macro Mechanical Assessment of Small – Intermediate Strain Properties of Granular Material" *Ph D Thesis, Faculty of Civil Engineering, Ruhr-U Bochum.*

[11] Feng, S.–Vardanega, P. J.–Ibraim, E.–Widyatmoko, I. –Ojum, C. (2018): „Permeability assessment of some granular mixture" *Géotechnique.*

Discussion

The structure of the grading curve space

Representing the space of the grading curves with N fractions by an N -1 dimensional, closed simplex, the A = constant condition means N -2 dimensional parallel hyper-planes in the Euclidean space generated by the simplex. The B = constant condition in addition is related to an N -3 dimensional, concentric topological circle around the optimal point on the A = constant hyper-plane section.

The optimal point is defined by the maximum of B for the given A value. The optimal point is close to the mass center of the A = constant hyper-plane simplex section.

The optimal grading curve is a kind of mean grading curve considering all grading curves with the same A. It is a fractal grading is with minimum arc length. Being the dimension of the optimal line (one) less than the dimension of the space of the grading curves (N-1), it is worthy to set up any relationship between the mean gradings (instead of the whole space of the grading curves) and a given physical parameter.

The grading entropy parameters are various statistical means. The base entropy S_0 is a kind of dimensionless mean log diameter, which is similar to d_m. Its normalized value the relative base entropy parameter A is a normalized mean log diameter, varying between 0 and 1 with a shift symmetry in the log diameter axis, the extremes are related to the minimum and maximum log diameters.

A indicates the relative distance of the mean and the minimum log d value. The base entropy S_0 is similar to dm. Its normalized value, the relative base entropy A is a continuous internal stability measure, the A<2/3 condition indicates internally (more) unstable soils (as A decreases).

The entropy increment ΔS and its normalized version B are log weighted generalized geometrical means of the x_j (j = 1, 2, 3...N), having maximum values of lnN/ln2 and 1/ln2, respectively. For those grading curves, in which all N fractions are well represented, the entropy increment is typically close to the maximum value. They reflect the actual effective number of fractions within the mixture (like the coefficient of uniformity c_u), and also reflect the degree of degradation.

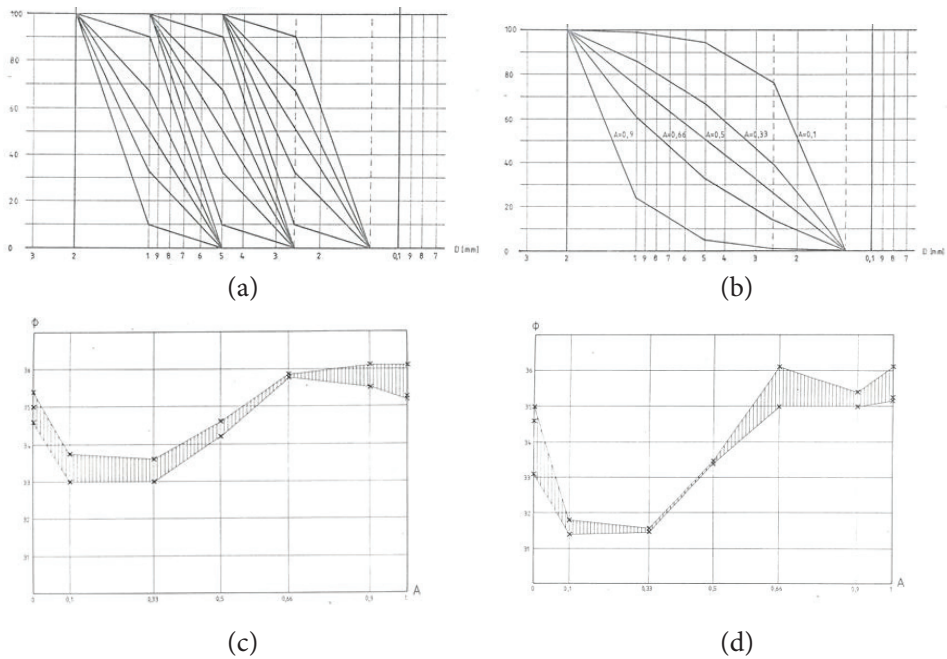
[1] Lőrincz J. (1986): "Grading entropy of soils," *Doctoral Thesis, Technical Sciences*. TU of Budapest (in Hungarian).

[13] Mitchell, J. K. (1976): *Fundamental of soil behavior.* London: Taylor & Francis.

[14] Thevanayagam, S. (1999): Intergranular contact and shear modulus of non-plastic granular mixes. In: *`13th ASCE Conference on Engineering Mechanics.* John Hopkins University.

[15] Göblyös, I. (1989): *The dependence of critical state friction angle on the entropy parameters.* MSc Thesis. Budapest: BME.

Figure 6. The relation of critical state friction angle and the entropy coordinate A in case of optimal sand soil mixtures ([15]). (a) and (b) grading curves of the 2-and 4-fraction sand mixtures. (c) and (d) critical state friction angle of the 2-and 4-fraction sand mixtures as A varies between 0 and 1.



The internal structure in terms of fines

The influence of fine particles on sand force structure, from micro-structure point of view, was first presented by Mitchell (1976) [13] and then simplifed by Thevanayagam (1998) [14] for other mechanical responses of transition soils. In two similar studies, the boundary between the "fines-in-sand" and "sand-in-fines" micro-structure was examined, and the threshold fines content was found at around A=2/3 [8, 9], supporting the internal stability criterion of. [1]

Critical state friction angle

Artificial - mixtures of natural sand grains (see Figure 6) were used to determine the critical state friction angle in [15]. The four fractions were: 0.125–0.25 mm, 0.25–0.5 mm, 0.5-1 mm, 1–2 mm (uniform distribution was assumed within the limits). The critical state friction angle measured on optimal 2-and 4-fraction soils are shown in Figure 6. Saturated, drained triaxial tests were made with sample dimension of 100mm diameter, 100 mm height until critical state. The samples were saturated after compaction. According to Figure 6, it was found that the critical state friction angle was dependent on A for each soil series in the same way. It can be noted that this dependence was similar to the dependence of the coordination number (see *Table 3)* but was not in agreement with the DEM critical state friction angle (see *Table 3*). Further research is suggested on this question, on the variation of the critical state friction angle in terms of the grading curve and the coordination number.

Conclusion

Originally the influence of fine particles on sand force structure, from micro-structure point of view, was examined [13, 14]. Lőrincz [1] generalized this idea to any grading curve using grading entropy parameter A, and connected it to internal stability of soils. The relative base entropy parameter A measures the distance between the mean and the minimum log diameters, varying between 0 and 1, it has a potential to be a criterion number for internal stability, based on the simple physical fact that if the mean grain diameter is large enough, then enough large grains are present in a mixture and these will form a stable skeleton. It follows from this sound physical basis that the two grading entropy coordinate pairs (normalized or non-normalized), proposed by Lőrincz [1] together with the integer variable N (the number of the fractions), S_{0min}– and d_{min}– (the entropy and diameter of the smallest fraction) may characterize the internal stability related phenomena like piping, liquefaction in terms of the grading curves more effectively than the usual diameter values. To establish relations between the entropy parameters and soil physical parameters are promising, real and DEM experiments are suggested to be performed and reevaluated in further research. Also, to describe soil degradation, soil modification, compaction or breakage both in laboratory and in nature condition, the grading entropy theory is useful tool.

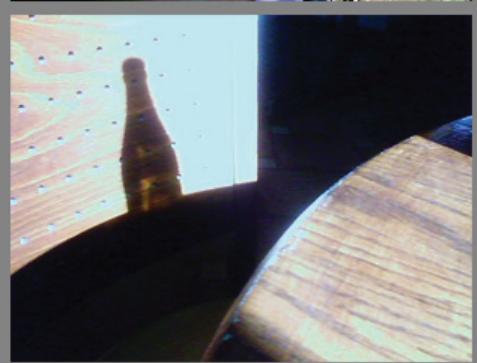
[1] Lőrincz J. (1986): "Grading entropy of soils," *Doctoral Thesis, Technical Sciences*. TU of Budapest (in Hungarian).

[13] Mitchell, J. K. (1976): *Fundamental of soil behavior.* London: Taylor & Francis.

[14] Thevanayagam, S. (1999): Intergranular contact and shear modulus of non-plastic granular mixes. In: *`13th ASCE Conference on Engineering Mechanics.* John Hopkins University.

[15] Göblyös, I. (1989): *The dependence of critical state friction angle on the entropy parameters.* MSc Thesis. Budapest: BME.







OROSZI ESZTER DIÁNA*

Biztonságtudatossági szabadulószoba, mint új programelem az információbiztonsági képzésekben

Összefoglaló: A biztonságtudatossági szabadulószoba a felhasználók információbiztonsági ismereteinek egy új fejlesztési eszköze, mely a „gamifikáció", játékosítás elemeivel segíti a munkavállalókat a biztonságtudatos magatartás elsajátításában és érzékenyíti őket a téma iránt. A program során a résztvevők olyan problémákkal és kockázatokkal találkozhatnak, melyeket akár ők, vagy munkakörnyezetük is alkalmazhat, és melyek egy potenciális támadó számára nagy segítséget jelenthetnek a károkozásban. A játékban való részvétellel a munkatársak gyakorlatilag tapasztalati úton ismerik fel a helytelen gyakorlatot és tanulják meg a biztonságtudatossági szemléletet, magatartást, ezért sokkal hatásosabbnak és hatékonyabbnak mondható, mint egy hagyományos tantermi vagy e-learning képzés.
Kulcsszavak: Social Engineering, biztonságtudatosság, szabadulószoba, információbiztonsági program, biztonságtudatossági kampány, speciális tréning, gamifikáció, játékosítás.

Abstract: Security awareness escape room is a new method of security awareness improvement. This program uses gamification elements to highlight information security risks and problems for users, for example bad habits of employees which could be exploited by a possible attacker. According to my experiences, users like the "learning-by-experience" better than classroom trainings, presentations or even online courses, because in this case participants can identify their own weaknesses and change their daily practices.
Keywords: Social Engineering, security awareness improvement, escape room, information security program, information security campaign elements, special training, gamification.

**Nemzeti Közszolgálati Egyetem, PhD-hallgató*
E-mail: eszter.oroszi@gmail.com

A szervezetek információbiztonsági területei egyre inkább felismerik a humán erőforrást kihasználó, Social Engineering jellegű támadások jelentőségét. Ahogyan Kevin Mitnick is állítja, a technológiai védelmi intézkedések nem elegendőek ezen típusú támadásokkal szemben. [1] Az egyetlen hatékony megoldás a munkavállalók biztonságtudatossági ismereteinek fejlesztése, érzékenyítése a téma iránt, ezért a biztonságtudatosság fokozása minden vállalat számára egyre fontosabb kell, hogy legyen, függetlenül attól, hogy milyen szektorban működik az adott szervezet. Ennek érdekében figyelemfelkeltő és hatékony biztonságtudatossági képzéseket és programokat kell szervezni a munkavállalók számára, melyek nem csak száraz oktatási anyagokat és szokványos kampányelemeket tartalmaznak az aktuális szabályok fókuszában, hanem rávilágítanak a valós problémákra is, például tesztek, auditok eredményeinek bemutatásával. [2] Jelen tanulmányban egy lehetséges módját mutatom be a biztonságtudatosságot fejlesztő programok fokozásának, a felhasználók érdeklődése felkeltésének.

A biztonságtudatossági képzések fő célja, hogy a munkavállalók megismerjék az információbiztonsági szabályzatból rájuk vonatkozó előírásokat, illetve azok meglétének, betartásának szükségességét. A tananyagoknak azonban nem csak ezen szabályok „unalmas" leírását kell tartalmazniuk, hanem annak bemutatását is, hogy miért is van ezekre szükség, milyen, az emberi tényezőt érintő támadási technikák léteznek (például fizikai bejutás az épületbe, adathalászat, kártékony kódok terjesztése és az internet egyéb veszélyei), melyek elkerüléséhez be kell tartani ezen előírásokat a kockázatok csökkentése érdekében. Tapasztalataim alapján azok az oktatások a leghatékonyabbak, melyekben való életből vett, akár helyi példákkal, fénykép- és videófelvételekkel színesítjük az előadást (akár megtörtént incidenst, akár egy biztonságtudatosság-mérést célzó Social Engineering audit eredményeit felhasználva). Ezen kívül érdemes az oktatásokat felhasználói szintenként megbontani és más, releváns, testreszabott tartalmat közvetíteni a vezetőség, az informatikai terület/üzemeltetés és az „átlagfelhasználók" részére. Természetesen amennyiben egyéb speciális csoport megkülönböztethető a szervezetnél (például titkárság, HelpDesk, ügyfélszolgálat, stb.), számukra is lehet dedikált tréninget tartani. A specializált anyagok segítik a résztvevő felhasználókat a valós veszélyek jobb megértésében, realizálásában és a védelmi intézkedések hatékonyabb elsajátításában. [3]

Amellett, hogy a felhasználók biztonságtudatossági szintjét rendszeresen mérjük és fejlesztjük különféle képzésekkel, nagyon fontos, hogy az ismereteket naprakészen tartsuk, illetve beépítsük a mindennapi életbe, így a felhasználók ténylegesen

[1] Mitnick, K. D. –Simon, W. L. (2003): *The Art of Deception – Contolling the Human Element of Security.* Wiley.

[2] Oroszi, E. D. (2019): *Security awareness escape room a possible new method in improving security awareness of users, Cyber Science Cyber Situational Awareness for Predictive Insight and Deep Learning*, C-MRiC.ORG. Oxford.

[3] Oroszi, E. D. (2018): *Social Engineering technikák, Célzott kibertámadások*. Budapest: Nemzeti Közszolgálati Egyetem.

alkalmazni tudják a tanultakat. Ennek egyik módja, ha rendszeresen biztonságtudatossági kampányokat is hirdetünk az oktatások kiegészítéseképpen, melyek segítenek a felhasználóknak visszaemlékezni a tanultakra a napi munkavégzés során is, fenntartják a figyelmet a biztonságtudatos magatartás iránt, valamint akár a gyakorlati tapasztalatszerzésre is lehetőséget adnak. Ezeken a biztonságtudatossági heteken vagy hónapokon a munkavállalók nem csak oktatásokon vehetnek részt, de találkozhatnak célzott előadásokkal, játékokkal, vagy akár az emberi tényezőt kihasználó támadásokra figyelmet felhívó poszterekkel, képernyőkímélőkkel, hírlevelekkel.

Amennyiben ezen akciósorozatok egy teljes évet átölelnek, már komplex biztonságtudatossági programról beszélhetünk. [3] Tapasztalataim alapján azonban nem egyszerű feladat egy olyan program vagy kampány összeállítása, mely tényleg hasznos ismereteket ad át a felhasználóknak, valamint ugyanakkor az érdeklődést is felkelti – például sokszor érkezett már olyan visszajelzés a kollégáktól, hogy már megint a helyes jelszó választására ösztönző plakát került kihelyezésre, holott a jelszavakkal kapcsolatos előírásokat már ismerik.

[3] Oroszi, E. D. (2018): *Social Engineering technikák, Célzott kibertámadások*. Budapest: Nemzeti Közszolgálati Egyetem.

Hagyományos és új elemek a biztonságtudatossági programok, kampányok során

A biztonságtudatossági kampányok célja a munkavállalók információbiztonsági ismereteinek felfrissítése, a tanultak felelevenítése, esetlegesen új információk megosztása (például elmúlt időszakban új támadási technika, trükk megjelenése), a kockázatok és szabályok felelevenítése az adott héten, hónapban vagy éppen egész éven át. A hagyományos programelemek közé sorolhatjuk a posztereket, képregényeket, melyek a fontosabb előírásokat mutatják be, képernyőkímélőket, ajándéktárgyakat (például egérpad, bögre, kulcstartó, póló, stb.), vagy akár használati tárgyakat is adhatunk logónkkal, mint például kameratakaró, jelszóképzést segítő kulcstartó, biztonságos bankkártyatartó, vagy akár játékok biztonságtudatos kiadása (például memóriakártya, Activity társasjáték, stb.).

Ezek sokszor kedves emlékeztetőt tartalmaznak, a munkatársak „jópofának" tartják őket, de nehéz megtalálni azokat az üzeneteket, melyektől nem lesznek unalmasak, és nem landolnak végül a kukában, vagy nem kerülnek továbbajándékozásra. Legtöbbször a probléma forrása az, hogy a felhasználók nem tudják, miért ezekkel az üzenetek-

kel találkoznak, az nem derül ki, mi történne, ha az adott szabályt nem alkalmaznák, nincsenek tisztában a kockázatokkal – ezért nagyon fontos cél, hogy ezek is visszaköszönjenek a programok során.

Hogyan lehet fejleszteni, feldobni a biztonságtudatossági kampányainkat? Alkalmazzunk szokatlan, egyedi, szervezetre szabott kampányelemeket, akár nyereményjátékok, gamifikáció alkalmazásával. Legegyszerűbb példa lehet mondjuk versengés a legbiztonságtudatosabb dolgozó címért, de lehet szervezni fotópályázatot biztonságtudatossági témában, melynek során mind a pályázók, mind a pályaművek megtekintői el tudnak gondolkodni a biztonságtudatosság fontosságán, az információbiztonságban betöltött szerepükön. Végül, de nem utolsósorban alkalmazhatunk olyan elemeket is, melyek a felhasználók aktív közreműködését igénylik, ilyen lehet például egy biztonságtudatossági szabadulószoba program meghirdetése, mely szintén alkalmazza az egyre divatosabb játékosítást. «A gamifikáció/játékosítás játékos elemeket és játékos gondolkodást alkalmaz 'nem játékos' környezetben, annak érdekében, hogy a célközönség viselkedését és elköteleződését fokozza." [4]

A klasszikus szabadulószobák nagyon népszerűek Magyarországon, ez adta a biztonságtudatossági szabadulószoba alapötletét. Hiszen ha oly sokan hajlandóak viszonylag magas összeget kifizetni egy órás csapatjátékért, a munkahelyeken ingyenesen biztosított biztonságtudatossági változat a munkavállalók számára is érdekes lehet. Emellett a játékosítás vállalati környezetben is egyre népszerűbb, sőt megjelentek már kifejezetten biztonságtudatossági játékok is (például online kvíz játékok, Cyber Jenga, stb.).

A biztonságtudatossági szabadulószobában végrehajtandó feladatok mindegyike valamely információbiztonsági ismerethez kötődik és tipikus hiányosságokra világít rá, fontos szabályokra hívja fel a figyelmet, például miért ne hagyjuk a kulcsunkat a ceruzatartóban, miért ne írjuk fel post-it-ekre a jelszavunkat, egyáltalán miért ne válasszunk egyszerű jelszót. Információbiztonsági tanácsadóként a kedvenc projektjeim a Social Engineering auditok és biztonságtudatossági képzések voltak, az ezek során szerzett tapasztalatok remekül beépíthetőek voltak a biztonságtudatossági szabadulószoba forgatókönyvekbe. Egyrészt jól lehetett azonosítani a tipikus biztonságtudatossági hiányosságokat, jellemző rossz szokásokat, másrészt az oktatásokon feltett kérdések, biztonságtudatossági kampányokra, programokra tett visszajelzések megalapozták egy érdekes és szokatlan program létrehozását. Véleményem szerint a felhasználók akkor érzik át az információbiztonság fontosságát, ha már megtörtént a baj (például incidens áldozatává válnak), illetve látják egy kockázat bekövetkezését – erre pedig a biztonságtudatossági szabadulószoba játékos környezete is alkalmas.

[4] Van den Boer, P. (2019): *Introduction to Gamification, Whitepaper,* https://cdu.edu.au/olt/ltresources/downloads/whitepaper-introductiontogamification-130726103056-phpapp02.pdf (letöltve: 15/01/2019)

A klasszikus és biztonságtudatossági szabadulószobák főbb különbségeit az alábbi táblázat mutatja be:

1. ábra. Különbségek a hagyományos és biztonságtudatossági szabadulószobák között.

Szempont	Klasszikus	Biztonságtudatossági
Tematika	Valóság-fikció széles skálája (kalóz, tudós, atomerőmű, utazó, gyilkos, stb.)	Valóság, elsősorban irodai környezet (titkárnő, főnök, projekt menedzser, stb.)
Cél	Szó szerint kiszabadulni, különben süllyed, robban, lelő, stb. ☺	A támadó bőrébe bújva hozzáférést szerezni a felhasználó számítógépéhez és megszerezni a fájl tartalmát
Feladatok jellege	Logikai, rejtvény, ügyességi	Biztonságtudatossági ismeretek
Résztvevők száma	2-6 fő	3-4 fő
Játékidő	60 perc	15-30 perc
Számítógép használat	Nem jellemző	Elengedhetetlen

Az első és legfontosabb különbség természetesen a forgatókönyv 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. 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 rendszergazdák 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.

Fontos különbség, hogy a hagyományossal ellentétben a biztonságtudatossági szabadulószobában nincsenek bezárva a játékosok, nem az a cél, hogy megtalálják a kijutást biztosító kulcsot. Itt ugyanis forgatókönyvtől függően a résztvevők vagy segítőkész munkatársak, akik pusztán jóindulatból szereznek meg egy fontos fájlt a «távol levő kolléga" számítógépéről, vagy éppen akár rosszindulatú támadók, akiknek célja a károkozás. Vagyis a cél az, hogy be tudjanak jelentkezni a fiktív személy számítógépébe és meg tudják

nyitni a kijelölt fájl – ez jelenti a «szabadulást" és a játék végét. Tekintve, hogy különbözőek a célok és a kerettörténetek, így természetesen az eszközök sem egyformák. Hagyományos esetben a feladatok logikai, ügyességi, kvíz jellegűek, akár konkrétan csapatjátékot is igényelve, ezzel szemben a biztonságtudatossági szabadulószoba kifejezetten információbiztonsági előírásokra, tudatossági elemekre épít, valós szokások köszönnek vissza (ugyan nem zárható ki egy-két hagyományos elem sem, de a fókusz nem ezeken kell, hogy legyen).

A biztonságtudatossági szabadulószoba jellemzően 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 választása
– alkalmazások biztonságtudatos használata (mind notebook-on, mind okostelefonon)
– titkosított adathordozók, titkosítási lehetőségek
– információmegosztás a közösségi médiában
– dokumentumok biztonságos megsemmisítése (mind papíralapon, mind elektronikusan)

Alapesetben egy normál szabadulószoba 2–6 játékossal 60 perc alatt oldható meg, egy biztonságtudatossági szabadulószoba esetében ugyanezen létszám mellett érdemes korlátozni az időt 15–30 percre, annak érdekében, hogy ne akadályozzuk jelentős mértékben a napi munkavégzést (illetve tapasztalat, hogy 30 perc után a forgatókönyv unalmassá válik, a játékosok elveszítik a korábbi érdeklődésüket, résztvevői visszajelzést idézve «akkor úgysem olyan nagy baj, ha nem vagyok biztonságtudatos, hiszen most sem sikerül megszerezni a fájlt".)

Végül az utolsó főbb különbség természetesen a számítógép-használat. Bár egyre több klasszikus szabadulószobában is megjelenik, hiszen például egy tudós professzor természetesen használhat IT-eszközöket, legtöbb esetben még mindig nem ezeken van a fő fókusz és a fikción alapuló forgatókönyveknél nem is jelenik meg. Ezzel szemben – tekintve, hogy fő feladat – a biztonságtudatossági szabadulószobának alapkellékei a számítógép, okostelefon, pendrive vagy más adathordozó. Természetesen maga a számítógép sem pusztán a fájl megnyitásának eszköze, azon keresztül is vannak megoldható feladatok, például elektronikus levelezés biztonságtudatos használata, közösségi média és egyéb alkalmazások használata.

A biztonságtudatossági szabadulószoba program megvalósítása

Amennyiben szabadulószobát tervezünk, ha van lehetőségünk, első lépésként próbáljuk meg azonosítani a munkatársak jelenlegi információbiztonsági ismereteit, hiányosságait, rossz szokásait, hogy 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 munkatársai ott tegyék, 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, 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.) Természetesen alkalmazhatunk általános forgatókönyvet, általános rossz példákkal (feladatokkal) is, azonban a program akkor a legizgalmasabb és hatásosabb, ha a résztvevők környezetére épül, hiszen általános esetben lehet, hogy nem is minden lesz releváns (például egyáltalán nem használnak jelszószéf megoldást a vállalatnál, holott a játékban szerepel).

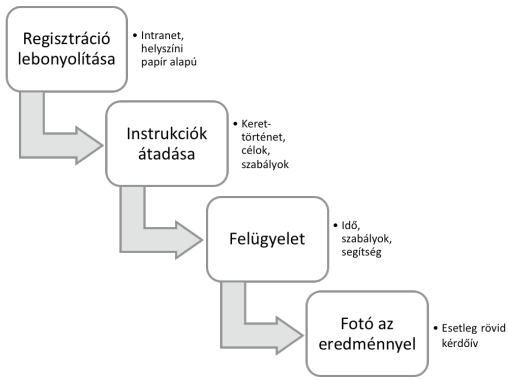
Ha megvan a forgatókönyvünk, karakterünk és a hiányosságokat bemutató feladatok váza, akkor érdemes még annyiban is vállalatra szabni, hogy azonosítjuk, milyen eszközöket használnak a szervezetnél és azokat építjük be, hiszen a különböző operációs rendszerek, szokatlan alkalmazások zavaróak, sőt akár akadályozóak is lehetnek a játék során (például ha a szervezetnél Windows-környezetben dolgoznak a felhasználók, egy Macbook nem lesz a legjobb választás a programhoz).

Ezt követően lehet létrehozni a fiktív felhasználót és előkészíteni a környezetét a virtuális térben is, például létrehozni a fiókját a Facebookon 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 csinálni, 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.

A biztonságtudatossági szabadulószoba program lebonyolításának lépéseit az alábbi ábra szemlélteti:

2. ábra. Biztonságtudatossági szabadulószoba program megvalósítása.



Miután megvan a végleges forgatókönyvünk és eszközeink, elkezdődhet a regisztrációs folyamat. A regisztrációs ívet feltehetjük virtuálisan egy online felületre, intranetre, de helyszíni regisztrációt is alkalmazhatunk papíralapon. Nagyon fontos, hogy bármelyiket is válasszuk, előzetesen kommunikáljuk ki a programot a munkatársak felé, hogy időben be tudják tervezni a napi munkavégzésbe. Amennyiben későn értesülnek róla a potenciális résztvevők, az is előfordulhat, hogy a program kudarcba fullad.
Javasolt, hogy a forgatókönyvet és játékszabályokat csak közvetlenül a játék elején osszuk meg a résztvevőkkel, ne kommunikáljuk ki előzetesen. Így egyrészt a lelkesebb résztvevőknek nincsen lehetősége előre dolgozni, másrészt így nem fogják elfelejteni a játék során.

Játékszabályok:
– Mondjuk el, mit tartalmaz a játéktér, meddig tart a fiktív iroda.
– Mondjuk el, milyen eszközök vannak, pl. WiFi, internet rendelkezésre áll, lehet használni.
– Mondjuk el, hogy mi a megnyitandó fájl neve, formátuma, milyen eszközön kereshetjük.
– Mondjuk el, privát eszközöket, például saját okostelefont lehet-e használni.
– Hívjuk fel a figyelmet arra, hogy csak biztonságtudatossági elemek hiányát kell felfedezni, hacker. trükköket nem kell alkalmazni (alapforgatókönyv esetén).
– Van-e pluszpont szerzési lehetőség.

– Kell-e vagy lehet-e felhasználót váltani a gépen.
– Speciális biztonsági szabályok, például „Forgot password" funkció törli a pendrive tartalmát, 10 sikertelen kísérlet után zárolásra kerül a fiók, stb.
– Kérjük meg a játékosokat, hogy ne változtassák meg a dokumentumok, fájlok tartalmát, valamint a beállításokat, illetve csak az erre kijelölt papíron jegyzeteljenek.
– Hívjuk fel a figyelmet arra, hogy a szemetest ne használják rendeltetésszerűen.

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 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 bizonyítványt, mely tartalmazza 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.

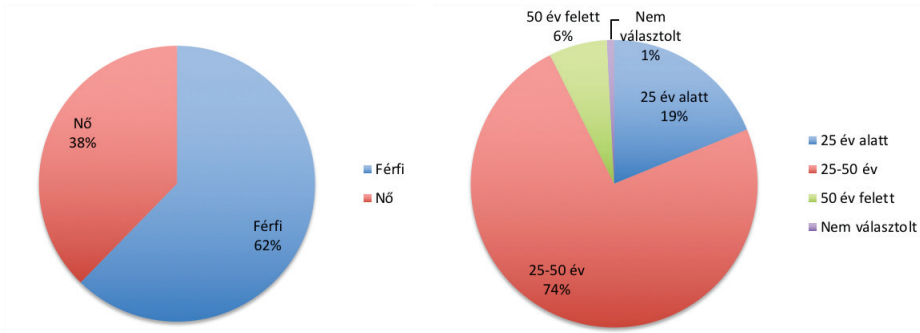
Az egyes játékoscsoportok között természetesen a játékmester feladata a rendrakás és annak ellenőrzése, hogy minden a normál állapotban maradt-e, vannak ugyanis vicces munkatársak, akik szeretik átírni például a jelszó-emlékeztetőt. Természetesen plusz pontként be lehet építeni a játékba a munkakörnyezet megóvását is.

Tapasztalatok

2014 és 2019 között összesen 120 biztonságtudatossági szabadulószoba játékot vezettem le különböző szervezeteknél és konferenciákon. Ez azt jelenti, hogy eddig körülbelül 600 személyt értem el ezzel az információbiztonsági programmal, két alkalommal külföldön is volt lehetőségem bemutatni a játékot. 2016-ban egy kérdőíves felmérést is folytattam, melynek során 230 résztvevő töltötte ki a kérdőívemet. [5]

[5] Oroszi, E. D. (2017): Biztonságtudatossági szabadulószoba, ISACA előadás, ISACA Hungarian Chapter, Budapest.

3–4. ábra. Résztvevői statisztikák nem és kor megoszlásban.



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.

A tapasztalatok és visszajelzések 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.

Az eddigi 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). 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. 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.).

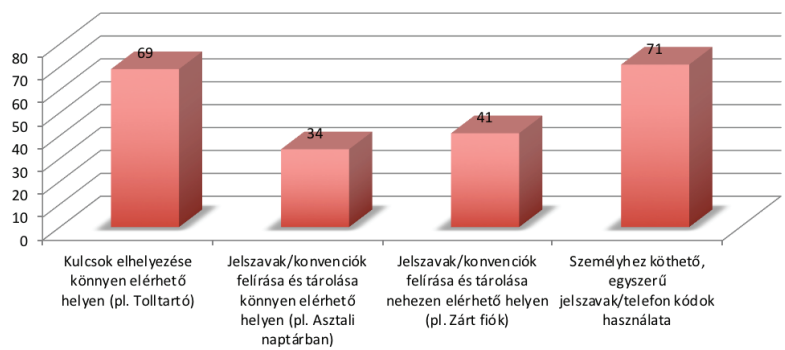
Többen ódzkodtak a mások (még ha csak fiktív személy) holmijai közötti turkálástól, ők bevallották, hogy nem gondolnák, hogy bárki is hozzá merne ily módon nyúlni a dolgaikhoz – jó tapasztalat volt látni

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 – nos, volt.

A külföldön szervezett játékok 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).

A 2016-os felmérésben kíváncsi voltam arra, hogy a résztvevők mely rossz szokásokat gyakorolják/gyakorolták saját bevallásuk szerint. Ahogyan feltételeztem, a kulcsok és a gyenge jelszóválasztás voltak a leginkább elkövetett hibák, ahogyan az alábbi diagram szemlélteti.

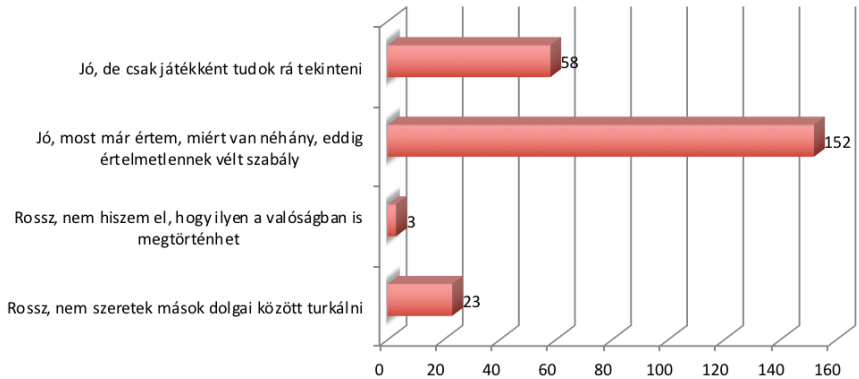
5. ábra. Mely hibákat követik el a játékosok is a való életben?



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 (3 fő) jelezte, hogy nem gondolja, hogy ilyen a való életben is előfordulhat.

[2] Oroszi, E. D. (2019): *Security awareness escape room a possible new method in improving security awareness of users, Cyber Science Cyber Situational Awareness for Predictive Insight and Deep Learning*, C-MRiC.ORG. Oxford.

6. ábra. Milyen érzésekkel távoztak a résztvevők a biztonságtudatossági szabadulószobából?



Összefoglalás

Összefoglalásként elmondható, hogy az eddigi tapasztalatok alapján a biztonságtudatossági szabadulószoba egy új és hatékony eszköze lehet az információbiztonsági képzéseknek, kampányoknak, hatékonyan képes fejleszteni a munkavállalók biztonságtudatossági szintjét. A játéknak olyan verziója is született 2019-ben, mely bevezette a «büntetés" vagy pontlevonás lehetőségét: amennyiben a játékos megnyitott a játék során például egy kártékony kódot szimuláló csatolmányt, a csapat időbüntetésben részesült. [2] Egyéb továbbfejlesztési lehetőségek is felmerültek, mint például az online játék, illetve mobiltelefonos applikáció-fejlesztés, illetve a irodai környezetben a többhelyszínes bevezetés (például egymás melletti irodák, teljes épülethasználat).

Galéria

Bakos Miklós fotói

