Dunakavics

A Dunaújvárosi Egyetem online folyóirata 2021. IX. évfolyam VII. szám

Műszaki-, Informatikai és Társadalomtudományok

Dunakavics

A Dunaújvárosi Egyetem online folyóirata 2021. IX. évfolyam VII. szám

Műszaki-, Informatikai és Társadalomtudományok

Megjelelenik évente 12 alkalommal

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

http://dunakavics.uniduna.hu/
ISSN 2064-5007

Tartalom

DUKAI KLÁRA *–NAGY BÁLINT **

Bizonyítások és analógiák

Összefoglalás: Az emberi gondolkodás, problémamegoldás sok esetben analógiákra épít. Jelen dolgozatban néhány bizonyítást mutatunk be, melyekben a felhasznált gondolatok nagyon hasonlítanak egy helyes tételre, de sajnos nem eléggé.
Kulcsszavak: Bizonyítás; ellenpélda; végtelen.

Abstract: In many cases, human thinking and problem solving is built on analogies. In the present work, some proofs are introduced in which the ideas used are very similar to a correct theorem, but unfortunately not enough.
Keywords: Proof; counterexample; infinity.

Bevezetés

A Dunaújvárosi Egyetem elkötelezett a hallgatóközpontú működés iránt. Ez abban is megnyilvánul, hogy a hallgatók véleménye alapján alakítja, fejleszti a kurzusait. Nincs ez másként a Matematika és Számítástudományi Tanszék által oktatott tantárgyak esetében sem. A matematika tárgyak hallgatói között 2020-ban végzett felmérések [1] más kutatásokkal együtt [2], [3], [4] rámutattak arra, hogy a hallgatók igénylik a szemléletes oktatási módszereket. Megállapíthatjuk azonban, hogy a szemléletesség és a pontosság nehezen egyeztethető össze. A kreativitás mellett [5], [6], [7] a pontosság – a matematika esetén kifejezetten – nélkülözhetetlen a sikerhez. A dolgozatban megfogalmazunk néhány állítást, (amelyek bizonyítása) valamely tétel, fogalom, eljárás nem megfelelő alkalmazása miatt hibás. Alábbiakban nem törekszünk arra, hogy a hibát részletesen tárgyaljuk, vagy a helyes eredmény eléréséhez szükséges matematikai fogalmakat részletesen leírjuk.

*Dunaújvárosi Egyetem, Informatikai Intézet
E-mail: duki@uniduna.hu

**Dunaújvárosi Egyetem, Informatikai Intézet
E-mail: nagyb@uniduna.hu

[1] Kocsó, E.–Cserné Pekkel, M.–Bognár, L.–Horváth, P. (2020): Matematika oktatása a Dunaújvárosi Egyetem levelező képzésein. *Journal of Applied Technical and Educational Sciences.* 10. (4.) Pp. 87–104.

[2] Erdélyi, K. (2010): Practice based course of Information Technology Service Management for BSc students In: *Teaching Mathematics and Computer Science.* 8. (2.) Pp. 229–246.

[3] Gogh, E.–Kovari, A. (2019): "Experiences of Self-regulated Learning in a Vocational Secondary School". *Journal of Applied Technical and Educational Sciences.* 9. (2.) Pp. 72–86.

[4] Szabó, Cs. M.: Can The Gap between Digital Natives and Digital Immigrants be Bridged in Education? (Áthidalható-e a szakadék az oktatásban a digitális bennszülöttek és a digitális beválndorlók között?) In: Hulyák-Tomesz Tímea (Ed.) (2019.): *Generációs kérdések a kommunikációs készségfejlesztésben.* Budapest: Hungaroox. Pp. 9–23.

[5] Kővári, A.–Rajcsányi-Molnár, M. (2020): Mathability and Creative Problem Solving in the MaTech Math Competition. *Acta Polytechnica Hungarica.* 17. (2.) Pp. 147–161.

[6] Váraljai, M. (2016): Establish innovative learning environment by virtual lab concept: An exploratory research in higher education, in 7th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), Wroclaw, Poland.

[7] Chmielewska, K.–Gilanyi, A. (2018): "Educational context of mathability," *Acta Polytechnica Hungarica.* 15. (5.) Pp. 223–237.

Célunk mindössze annyi, hogy megmutassunk a hamis bizonyítások közül néhányat, melyek több szempontból érdekesek.

Az első

Tétel: $$\frac{16}{64}=\frac{1}{4}.$$

„Bizonyítás": Vegyük észre, hogy a 6-os számjegy a számlálóban és a nevezőben is szerepel, így egyszerűsíthetünk vele:

$$\frac{16}{64}=\frac{1\cancel{6}}{\cancel{64}}=\frac{1}{4}.$$

A „Bizonyítás" elemzése:
Természetesen a „Bizonyítás" botorság. A – mindenki által tanult – egyszerűsítés nem így működik. Egy tört akkor egyszerűsíthető, ha a számlálója és nevezője szorzattá alakítható, melyekben van közös tényező. Ezzel a közös tényezővel lehet egyszerűsíteni.
A 16/64 számlálója és nevezője szorzattá alakítható a jól ismert prímtényezőkre bontás módszerével.

16	2
8	2
4	2
2	2
1	

és

64	2
32	2
16	2
8	2
4	2
2	2
1	

tehát $16=2^4$ és $64=2^6$.
Így az egyszerűsítés helyesen:

$$\frac{16}{64}=\frac{2^4}{2^6}=\frac{2\cdot2\cdot2\cdot2}{2\cdot2\cdot2\cdot2\cdot2\cdot2}=\frac{\cancel{2}\cdot\cancel{2}\cdot\cancel{2}\cdot\cancel{2}}{\cancel{2}\cdot\cancel{2}\cdot\cancel{2}\cdot\cancel{2}\cdot2\cdot2}=\frac{1}{2\cdot2}=\frac{1}{4}.$$

Érdekes, hogy bár a „Bizonyítás" téves, ebben az esetben az eredmény mégis helyes.

A második

Tétel:

$$5=7$$

„Bizonyítás”:
Két kifejezés egyenlőségének bizonyítására szép módszer, ha az egyik oldalon szereplő kifejezésből kiindulva azonos átalakítások sorozatát hajtjuk végre addig, míg a másik oldalon szereplő kifejezéshez jutunk. Induljunk most ki a bal oldalon álló kifejezésből, s alkalmazzuk a négyzetgyök definícióját

$$5 = \sqrt{25}$$

A 25 felírható 16 és 9 összegeként, így

$$\sqrt{25} = \sqrt{16 + 9}$$

A négyzetgyökről tanultak szerint

$$\sqrt{16 + 9} = \sqrt{16} + \sqrt{9}$$

Itt a négyzetgyök definíciója szerint haladhatunk tovább, s kapjuk

$$\sqrt{16} + \sqrt{9} = 4 + 3 = 7.$$

Ezzel a bizonyítást befejeztük.

A „Bizonyítás” elemzése.
Az első lépés a négyzetgyök definíciója szerint helyes, $5 = \sqrt{25}$. Természetesen a 25 felbontható a 16 és a 9 összegére, így a második lépés is helyes. A harmadik lépés azonban hibás. Az itt alkalmazott azonossághoz csak formálisan hasonló van: Ha a és b pozitív valós számok, akkor $\sqrt{a \cdot b} = \sqrt{a} \cdot \sqrt{b}$ amint ezt középiskolában mindenki tanulta.
Ebben a „Bizonyításban” az vezetett tévútra, hogy egy közismert azonosság felületes megjegyzése $(\sqrt{a \cdot b} = \sqrt{a} \cdot \sqrt{b})$ alapján egy ahhoz hasonlót, annak egy hamis analógiáját $(\sqrt{a + b} = \sqrt{a} + \sqrt{b})$ alkalmaztuk.

A harmadik

Tétel:

$2 \cdot 2$ néha 5.

„Bizonyítás”
Tudjuk, hogy $2 \cdot 2=2+2=4$. Felhasználjuk továbbá a gyökvonásról tanultakat

$$2 \cdot 2 = 2 + 2 = 4 - \frac{9}{2} + \frac{9}{2} = \sqrt{\left(4 - \frac{9}{2}\right)^2} + \frac{9}{2} =$$

Alkalmazhatjuk a két tag különbségének négyzetéről tanult
$(a\text{-}b)^2=a^2\text{-}2 \cdot a \cdot b+b^2$ azonosságot, így

$$\sqrt{\left(4 - \frac{9}{2}\right)^2} + \frac{9}{2} = \sqrt{4^2 - 2 \cdot 4 \cdot \frac{9}{2} + \left(\frac{9}{2}\right)^2} + \frac{9}{2} = \sqrt{-20 + \left(\frac{9}{2}\right)^2} + \frac{9}{2} =$$

Itt a -20 felírható 25-45 alakban.

$$\sqrt{-20 + \left(\frac{9}{2}\right)^2} + \frac{9}{2} = \sqrt{25 - 45 + \left(\frac{9}{2}\right)^2} + \frac{9}{2} =$$

Mivel $25=5^2$ és $45=2 \cdot 5 \cdot 9/2$,

$$\sqrt{25 - 45 + \left(\frac{9}{2}\right)^2} + \frac{9}{2} = \sqrt{5^2 - 2 \cdot 5 \cdot \frac{9}{2} + \left(\frac{9}{2}\right)^2} + \frac{9}{2} =$$

Ismét alkalmazható a két tag különbségének négyzetéről tanult azonosság:

$$\sqrt{5^2 - 2 \cdot 5 \cdot \frac{9}{2} + \left(\frac{9}{2}\right)^2} + \frac{9}{2} = \sqrt{\left(5 - \frac{9}{2}\right)^2} + \frac{9}{2} = 5 - \frac{9}{2} + \frac{9}{2} = 5,$$

amit bizonyítani kellett.

A „Bizonyítás" elemzése:
Természetesen a négyzetgyök alkalmazása hibás. Amint megtanultuk középiskolában, minden valós a szám esetén $\sqrt{a^2} = |a|$, s így a fent alkalmazott

$$4 - \frac{9}{2} = \sqrt{\left(4 - \frac{9}{2}\right)^2}$$

hibás. Helyesen

$$4 - \frac{9}{2} = \frac{8}{2} - \frac{9}{2} = -\frac{1}{2} \neq \sqrt{\left(4 - \frac{9}{2}\right)^2}.$$

Így – nem csalás, nem ámítás – a $2 \cdot 2$ néha 5 csak a filmtörténelemben marad helyes.

A negyedik

Tétel:

$$2=1$$

„Bizonyítás:"
Legyen $x \neq 0$ tetszőleges valós szám. Ekkor nyilván

$$x^2 - x^2 = x^2 - x^2$$

Az egyenlet bal oldalán álló kifejezésre alkalmazható a középiskolából jól ismert azonosság, $a^2 - b^2 = (a + b) \cdot (a - b)$, így $x^2 - x^2 = (x+x) \cdot (x - x)$. Ezt beírva:

$$(x + x) \cdot (x - x) = x^2 - x^2$$

Az egyenlet jobb oldalán szereplő kifejezés x kiemelésével átalakítható, így $x^2 - x^2 = x \cdot (x - x)$

$$(x + x) \cdot (x - x) = x \cdot (x - x)$$

Nyilván oszthatunk az egyenlet mindkét oldalán megtalálható kifejezéssel:

$$x + x = x$$

A bal oldalon összevonás után

$$2x = x$$

Végül

$$2 = 1,$$ amit bizonyítani kellett.

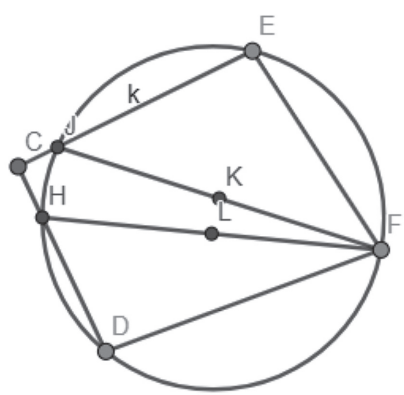
A „Bizonyítás" elemzése.
Természetesen itt is egy lépés pongyola kivitelezése okozta a problémát. Az egyenletek megoldásánál gyakran alkalmazott mérlegelv szerint csak akkor szabad az egyenlet mindkét oldalát osztani, ha az osztó nem nulla. Jelen esetben az x - x kifejezés nyilván nulla.

Az ötödik

Tétel: Létezik olyan kör, amelynek legalább két középpontja van.

„Bizonyítás:"
Tekintsük az *1. ábra* szerint a *k* kört, s annak egy *C* külső pontját. Legyen továbbá *D* és *E* a *k* kör két különböző pontja. Állítsunk merőlegest a *CD* és *CE* szakaszokra. Ezek a merőlegesek a *k* kör *F* pontjában metszik egymást. Jelölje a *CE* szakasz és a *k* kör közös pontját *J*, és a *CD* szakasz és a k kör metszéspontját H. A JF szakasz a kör *E* pontjából derékszögben látszik, így Thalesz tétele szerint a *JF* szakasz *K* felezőpontja a k kör középpontja. Hasonlóan a *HF* szakasz derékszögben látszik a k kör *D* pontjából, így Thalesz tétele szerint a *HF* szakasz *L* felezőpontja a k kör középpontja. Így a *k* körnek a *K* és *L* különböző pontok mindegyike a középpontja. Tehát a *k* körnek legalább két középpontja van.

1. ábra. A kör, amelynek két középpontja van



A „Bizonyítás" elemzése:
A „Bizonyítás" természetesen hibás. A többször is említett Thalesz tétel szerint ugyanis, ha *CEF∠=90°* és az *FDC∠=90°*, akkor az F pont nem illeszkedik a k körre.

A hatodik

Tétel:

$$0,\dot{9} < 1.$$

„Bizonyítás": A $0,\dot{9}$ egészrésze 0, ami kisebb 1-nél, így az állítás nyilvánvaló.

A „Bizonyítás" elemzése:
A Tétel állítása valójában hibás, bár ez sokak számára meglepő. Legyen ugyanis $A = 0,\dot{9}.$
A középiskolában tanult módszerrel írjuk fel *A*-t törtalakban.

$$\left.\begin{aligned} A &= 0{,}9999\ldots \\ 10A &= 9{,}9999\ldots \end{aligned}\right\}$$

Vonjuk ki a második egyenlőségből az elsőt:

$$9A=9$$

Így

$$A=1.$$

Másik módszert is alkalmazhatunk annak bizonyítására, hogy $0,\dot{9} = 1.$

$$0,\dot{9} = 0{,}9999\ldots = \frac{9}{10} + \frac{9}{100} + \frac{9}{1000} + \frac{9}{10000} + \cdots$$
$$= \frac{9}{10} + \frac{9}{10}\cdot\frac{1}{10} + \frac{9}{10}\cdot\frac{1}{100} + \frac{9}{10}\cdot\frac{1}{1000} + \cdots =$$

Felhasználva, hogy

$$\lim_{n\to\infty}(1 + q + q^2 + q^3 + \cdots) = \frac{1}{1-q}, \text{ ha } |q| < 1.$$

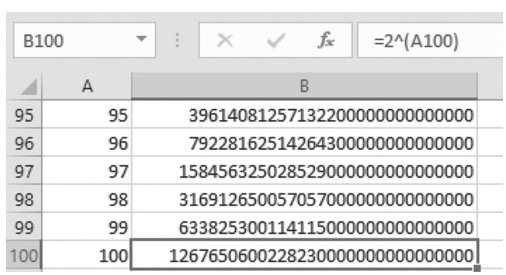
$$\frac{9}{10}\cdot\left(1+\frac{1}{10}+\left(\frac{1}{10}\right)^2+\left(\frac{1}{10}\right)^3+\cdots\right)=\frac{9}{10}\cdot\left(1+\frac{1}{10}+\left(\frac{1}{10}\right)^2+\left(\frac{1}{10}\right)^3+\cdots\right)$$
$$=\frac{9}{10}\cdot\frac{1}{1-\frac{1}{10}}=1.$$

A hetedik

Tétel:
2^{100} utolsó számjegye 0.

„Bizonyítás:”
Számítógéppel, bizonyos táblázatkezelő program alkalmazásával bizonyítható a fenti állítás:
Az első, A oszlopba írjuk a pozitív egészeket. A második oszlopba pedig 2 megfelelő hatványának értékét számítjuk ki a táblázatkezelő segítségével. A B3 cellába tehát például „=2^(B3)” kerül, s mivel $2^3=8$, így a B3 cellában a 8 látható. A képlet másolásával az *2. ábra* szerinti eredmény látható, amely alapján az állítás nyilvánvaló.

2. ábra. A 2 „hatványai”



A „Bizonyítás" kapcsán néhány gondolat:
Vizsgáljuk 2 hatványait: $2^1=2$, $2^2=4$, $2^3=8$, $2^4=16$, $2^5=32$, $2^6=64$, … Megállapítható, hogy a hatványokban az utolsó jegyek ismétlődnek: 2, 4, 8, 6, 2, 4, 8, 6,…., azaz 4 különböző végződés ismétlődik ebben a sorrendben. Mivel $100=25 \cdot 4$, ezért a 2^{100} utolsó jegye megegyezik 2^4 utolsó jegyével, tehát a keresett utolsó számjegy 6.

A nyolcadik

Tétel:

$$1=-1.$$

Az $1=(-1) \cdot (-1)$ miatt nyilván írható, hogy $1 = \sqrt{1} = \sqrt{(-1) \cdot (-1)}$.

A gyökvonás ismert azonossága $\sqrt{a \cdot b} = \sqrt{a} \cdot \sqrt{b}$ szerint $\sqrt{(-1) \cdot (-1)} = \sqrt{-1} \cdot \sqrt{-1}$.

A négyzetre emelés felírható: $\sqrt{-1} \cdot \sqrt{-1} = \left(\sqrt{-1}\right)^2$.

A négyzetgyök $\sqrt{a}^2 = a$ értelmezése szerint pedig $\left(\sqrt{-1}\right)^2 = -1$.
Tehát az alábbi átalakításokat végeztük:

$$1 = \sqrt{1} = \sqrt{(-1) \cdot (-1)} = \sqrt{-1} \cdot \sqrt{-1} = \left(\sqrt{-1}\right)^2 = -1$$

Végül megállapíthatjuk, hogy az egyenlőkkel egyenlők egymással is egyenlők, így $1=-1$.

Természetesen a fenti levezetésben több alkalommal nem használtuk az azonosságok és tételek feltételeit. Például a négyzetgyök értelmezése nyilván nem akármilyen *a* valós szám esetén tehető meg. A négyzetgyök definícióját pontosan az ilyen pongyola és félrevezető alkalmazások miatt középiskolában az alábbiak szerint szokás megfogalmazni:

Legyen az a nemnegatív valós szám. Ekkor $\sqrt{a}$ jelenti azt a nemnegatív valós számot, aminek négyzete ***a***.
Negatív valós számok négyzetgyökét nem definiáltuk.

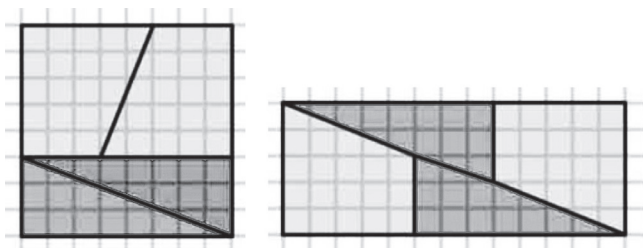
A kilencedik

Tétel:

64=65

A *3. ábrán* látható vázlat szerint egy 8x8-as négyzet átdarabolható egy 5x13-as téglalappá, ami bizonyítja állításunkat.

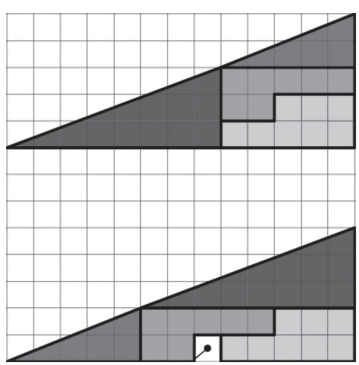
3. ábra. Négyzet átdarabolása



https://puzzling.stackexchange.com/questions/24848/how-can-64-65 (2021. január 10.)

Hasonló eredményre juthatunk a *4. ábra* felhasználásával is:

4. ábra. Háromszög átdarabolása



[http://www.erdekessegek.hu/index2_27.htm] 2021. január 10.

A tétel más megfogalmazásban a végtelen csokoládé paradoxonaként is ismert (https://www.youtube.com/watch?v=dmBsPgPu0Wc (2021. február 4.).

Számos bizonyítás során valamely alakzat feldarabolását egy másik alakzattal hozunk fedésbe, így bizonyítva, hogy a két alakzat területe azonos.

Hasonlóan szemléltethető (bizonyos *a*-ra és *b*-re) a közismert

$$(a + b)^2 = a^2 + 2ab + b^2,$$

az

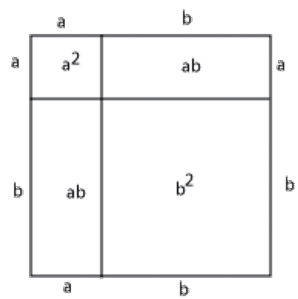
$$(a + b)(a - b) = a^2 - b^2$$

és az

$$(a + b)^3 = a^3 + 3a^2 b + 3ab^2 + b^3$$

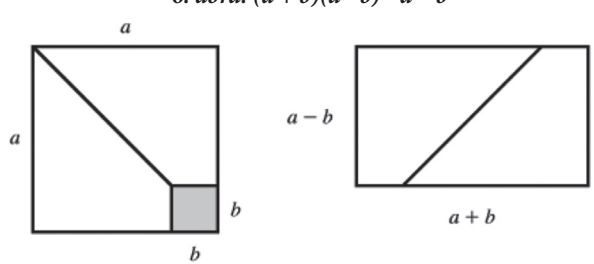
azonosság is.

5. ábra. $(a + b)^2 = a^2 + 2ab + b^2$



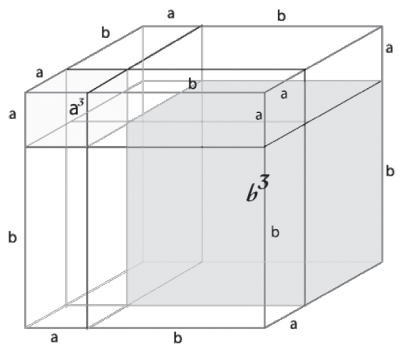
https://tudomanyplaza.hu/nevezetes-azonossagok/ 2021. január 10.

6. ábra. $(a + b)(a - b) = a^2 - b^2$



https://matkonyv.fazekas.hu/chapter.php?mode=s-ehs-j-&volume=a_i&code=A.I&chapter=chs_a_i/a_i_nevazon&chapternum=16&topic=Algebra&yearpair=7--8 (2021. január 10.)

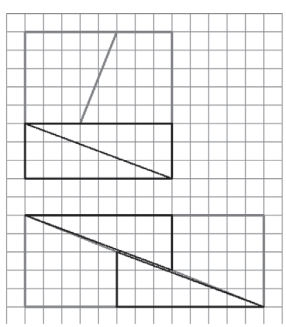
7. ábra. $(a + b)^3 = a^3+3a^2 b + 3ab^2 + b^3$



https://tudomanyplaza.hu/nevezetes-azonossagok/ 2021. január 10.

A „Bizonyítás" cáfolata:
Hasonlóan szemléletes, ám sokkal precízebb ábra cáfolja a fenti állítást: *8. ábra.*

8. ábra. Jól látható, hogy a téglalap esetében a háromszög oldala nem a téglalap átlóján nyugszik. Innen származik a további egy kis négyzet. (8·8+1=5·13.)



https://puzzling.stackexchange.com/questions/24848/how-can-64-65 (2021. január 10.)

Összefoglalás

Jelen dolgozatban néhány szemléletes bizonyítást és az ezeken alapuló tévedéseket mutattunk be.

KOCSÓ EDINA *–NAGY BÁLINT **

GeoGebra a matematika oktatásában és kutatásában

Összefoglalás: A matematika az egyik legelvontabb tudomány, így oktatásához, tanulásához minden lehetséges szemléltető eszköz alkalmazása célszerű. Míg adott iskolafokon megfelelő szemléltető eszköz lehet a kézzel fogható matematikai modell, bizonyos fogalmak oktatásához hasznos lehet egy multimédiás animáció. Jelen dolgozatban a többek között matematikai fogalmak szemléltetésére vagy kutatási feladatok megoldására egyaránt használható, GeoGebra programcsomag által kínált néhány lehetőséget tárgyaljuk.
Kulcsszavak: Matematikaoktatás; GeoGebra; szemléltetés.

Abstract: Mathematics is one of the most abstract sciences, so it is advisable to use all possible illustrative tools for teaching and learning. While a tangible mathematical model may be a suitable illustrative tool at a given school level, a multimedia animation may be useful for teaching certain concepts. In this work, we discuss some of the possibilities offered by the GeoGebra software package, which can be used to illustrate mathematical concepts or solve research tasks.
Keywords: Mathematics education; GeoGebra; illustration.

Bevezetés

Egy megfogalmazás szerint a matematika annyira elvont tudomány, minden lehetőséget meg kell ragadni ahhoz, hogy minél szemléletesebben lehessen tanulni. [1], [2], [3]

Különböző oktatási felfogásoknak megfelelően különböző szemléltetési módok alakultak ki.

**Dunaújvárosi Egyetem, Tanárképző Központ*
E-mail: kocsoe@uniduna.hu

***Dunaújvárosi Egyetem, Informatikai Intézet*
E-mail: nagyb@uniduna.hu

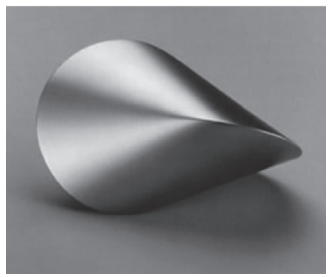
[1] Kővári, A.–Rajcsányi-Molnár, M. (2020): Mathability and Creative Problem Solving in the MaTech Math Competition. *Acta Polytechnika Hungarica,* 17. (2.) Pp. 147–161.

[2] Váraljai, M. (2016): Establish innovative learning environment by virtual lab concept: An exploratory research in higher education, in 7th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), Wroclaw, Poland.

[3] Chmielewska K.–Gilanyi, A. (2018): Educational context of mathability, *Acta Polytechnica Hungarica.* 15. (5.) Pp. 223–237.

Az oloid *(1. ábra.)* szemléltetésére például bizonyos felfogás követői a test modelljét mutatják meg.

1. ábra. Oloid [4]



Mások a gyerekekkel együtt gyurmából formázzák meg a testet. Vannak, akik egészen sajátos módon *(2. ábra.)* mutatják be ennek a speciális geometriai formának néhány jellegzetes tulajdonságát.

2. ábra. Oloid szemléltetése [5]

A GeoGebra

Az egyik legismertebb dinamikus geometriai és algebrai oktatóprogram a GeoGebra. Napjainkban egészen megszokott módon, a számítógép és az internet segítségével kínál néhány igen jól használható megoldást a matematikát szemléltetni kívánó oktatóknak. A GeoGebra neve a geometria és az algebra szavakból származik, mivel a program által kezelt objektumokat geometriai és algebrai úton is definiálhatjuk. A programot

[4] https://www.youtube.com/watch?v=GUyou2QelRo (2021. január 6.)

[5] http://math-exhibit.com/oloid/ (2021. január 6.)

kezdetben Markus Hohenwarter és csapata fejlesztette a Salzburgi Egyetemen, az idők során azonban a használók népes táborából egy olyan közösség alakult ki, akik aktív munkájukkal közösen alakítják a programot és kínálnak számos oktatási segédanyagot a világ számos pontjáról. [6] A program egy geometriai rendszer, ahol pontokat, vektorokat, szakaszokat, egyeneseket, kúpszeleteket éppúgy ábrázolhatunk, mint függvényeket, s ezeket az objektumokat később dinamikusan változtathatjuk is. Megadhatunk közvetlenül egyenleteket és koordinátákat is, illetve változóként használhatunk számértéket, pontot, vektort. A GeoGebra képes a függvények deriváltjának és integráljának meghatározására, valamint parancsokat biztosít a gyökök és szélsőértékek kereséséhez. GeoGebra előnye, hogy az alakzat egyszerre van jelen kifejezés és geometriai alakzat formájában.

[6] Hohenwarter M., http://www.geogebra.org (2021. január 6.)

A GeoGebra ingyenesen elérhető, nyílt forráskódú, továbbá platform-független. Futtatásának egyetlen feltétele a Java környezet, amely szintén ingyenes. A GeoGebra mellett szól még az is, hogy magyar nyelven is elérhető.

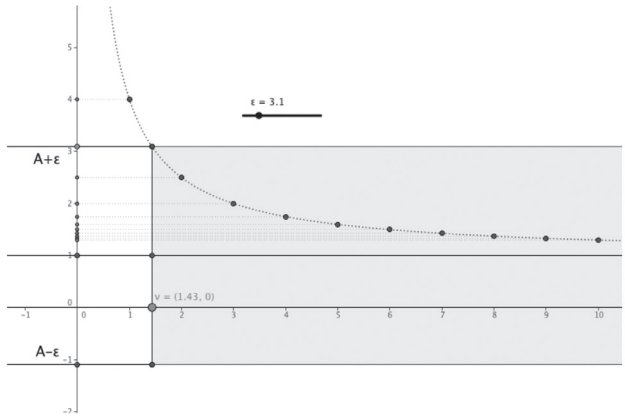
Bizonyos változókat ún. csúszka segítségével tudunk definiálni. Ha például egy változtatható sugarú kört szeretnénk rajzolni, akkor először a kör sugarának készítünk egy csúszkát. Ezen megadjuk a kör sugarának a nevét (r), majd megadjuk azt az intervallumot, ahol a kör sugara értéket vehet fel, végül középpontjával és sugarával megadunk egy kört, és a sugár hosszát r-nek definiáljuk. Ezáltal r változtatásával az ábrázolt kör sugara is változik.

A GeoGebra lehetőségeinek kihasználásával dinamikusan változtatható szemléltető animációkat készítettünk, mely a matematikai analízis néhány fogalmának oktatásához nyújt segítséget. A gyűjteménybe az analízis tanulása során felmerülő fogalmak, definíciók, tételek jelentését magyarázó, szemléltető dinamikus ábrák kerültek. A dolgozat további fejezeteiben ezen animációk közül mutatunk be néhányat.

Sorozatok határértéke

Mint közismert, az $\{a_n\}$ sorozat konvergens, ha létezik egy $A \in R$ valós szám, hogy bármely $\varepsilon>0$ esetén megadható olyan ν küszöbszám, hogy ha $n>\nu$, akkor a_n-nek A-tól való eltérése kisebb, mint ε, azaz $|a_n-A|<\varepsilon$.

3. ábra. A sorozatok határértékének oktatásához készített animáció képernyőképe



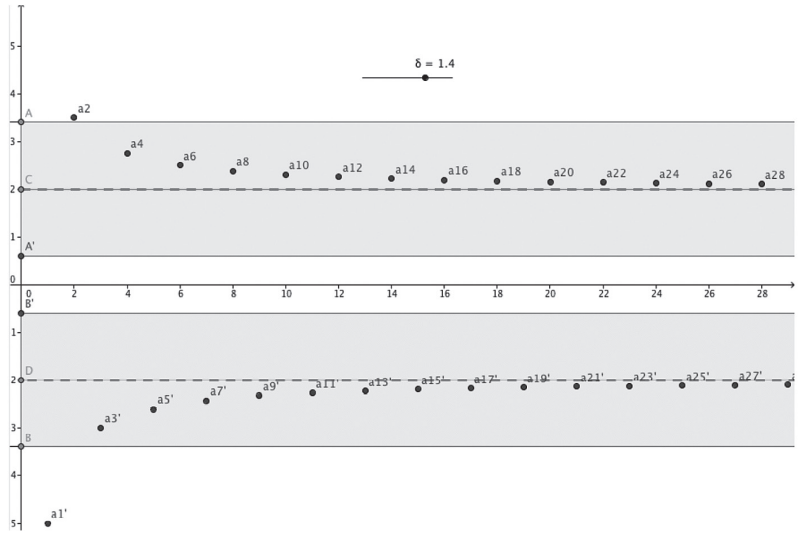
A *3. ábrán* többek között az $a_n=1+3/n$ sorozat első tíz tagját ábrázoltuk. A koordináta-rendszer *x* tengelyén *n*, míg az *y* tengelyén a_n értékei láthatóak. Az ábra alapján könnyen sejthető, hogy a sorozat határértéke $A=1$. Az ε értéke csúszkán állítható. Így könnyen megmutatható, hogy tetszőleges pozitív ε-hoz található ν. Például tekintsük az ε=2,1 esetet. Az animáción látható az A valós szám ε sugarú környezete, azaz a $(A+\varepsilon; A-\varepsilon)$ intervallum. A sorozat első tagja a jelölt sávon kívül van. A 2. tag viszont $a_2=2,5$, így *A*-tól való távolsága 1,5, azaz 2,1-nél közelebb van *A*-hoz, így benne van az *A* ε sugarú környezetében, a piros sávban. Jól látható, hogy a 2 indexű sorozattagtól kezdve az összes tag benne van ebben a környezetben. Az ábráról $\nu\approx1,4$ is leolvasható.

Torlódási pont

Azt mondjuk, hogy az $\{a_n\}$ sorozat torlódási pontja a $T\in R$ szám, ha *T* bármely környezetében a sorozatnak végtelen sok tagja található.

Például tekintsük az $a_n=(-1)^n\cdot(2+1/n)$ sorozatot. A *4. ábrán* a sorozat első néhány tagját ábrázoltuk. A csúszkával a δ értéket változtatva szűkíthetjük, illetve bővíthetjük a vizsgált környezetet. Jól látható, hogy a sorozatnak két torlódási pontja van. A páros *n* esetén a 2-höz, a páratlan *n* esetén pedig a -2 -höz tart a megfelelő részsorozat.

4. ábra. Sorozat torlódási pontját szemléltető animáció képe

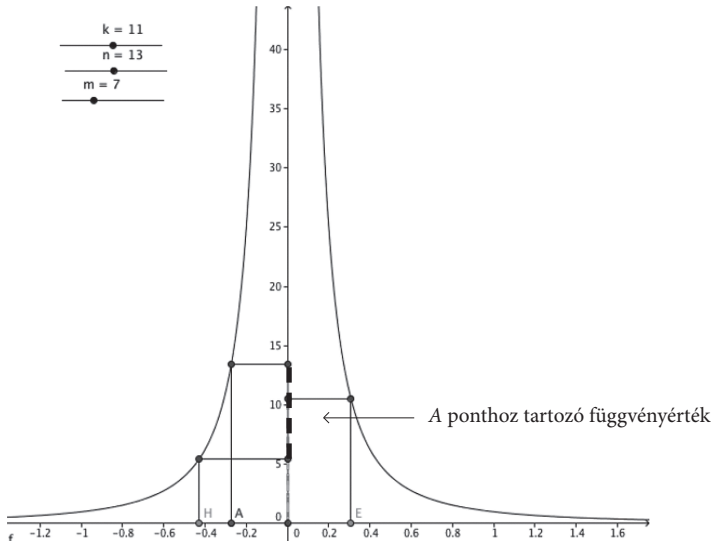


Függvény határértéke

A függvények határértékét több definíció segítségével is megadhatjuk. Alább a Heine-féle definíció szemléltetéséhez alkalmazott ábrát tekintjük. A definíció szerint:

Legyen az f függvény az x_0 pont valamely környezetében értelmezett, kivéve esetleg az x_0 pontot. Ekkor az f függvénynek az x_0 pontban $+\infty$ a határértéke, ha bármely $x_n \to x_0$ $(x_n \in D_f, x_n \neq x_0)$ sorozatra a függvényértékek sorozata végtelenhez tart, azaz $f(x_n) \to +\infty$.

5. ábra. Az R\{0}→R, x↦1/x² függvény szemléltetése a GeoGebra segítségével



Az R\{0}→R, x↦1/x² függvény 0 pontbeli határértékét szemléltetjük a GeoGebra program segítségével. A fenti definíciónak megfelelően három különböző sorozattal közelítjük meg az $x_0 = 0$ pontot. A három sorozat elemeinek indexeit a három csúszkával tudjuk megadni. Például az n csúszka az E pont koordinátáit határozza meg. Midőn a csúszkán n értékét változtatjuk, az *E* pont koordinátái: (*4/n; 0*) is változnak.

Az első esetben *E* pont tart a 0-hoz, mert első koordinátája – a *4/n* – az n növelésével tart 0-hoz. Ezáltal azokat a sorozatokat szemléltetjük, melyek szigorúan monoton csökkenő módon tartanak 0-hoz. Az *E* pont első koordinátája az R\{0}→R, x↦1/x² függvény értelmezési tartományában van, így meghatározhatjuk az *E*-hez tartozó függvényértéket, amit az *y*-tengelyen barna szaggatott vonallal jelöltük. Az *n* növelésével a függvény értéke a végtelenbe tart. A csúszkán történő mozgatással párhuzamosan látják a hallgatók, hogy a függvényértékek hogyan nőnek és tartanak a végtelenhez.

A *H* ponthoz tartozó értéket zöld szaggatott vonallal jelöltük. Csúszkával az *m*-et növelve a függvényérték tart a pozitív végtelenbe. A *H* ponttal szemléltetjük mindazokat a sorozatokat, melyek szigorúan monoton növekvő módon tartanak 0-hoz, hiszen *H* koordinátái (*- 3/m; 0*).

Az *A* ponttal szemléltetjük mindazokat a sorozatokat, melyek oszcillálva tartanak 0-hoz, hiszen koordinátái ($(-1)^k$ *3/k; 0*). Az *A* ponthoz tartozó függvényérték az ábrán jelölve van. A k csúszka állításával a pont első koordinátája negatív és pozitív értékek közt váltakozik a szorzónak köszönhetően.

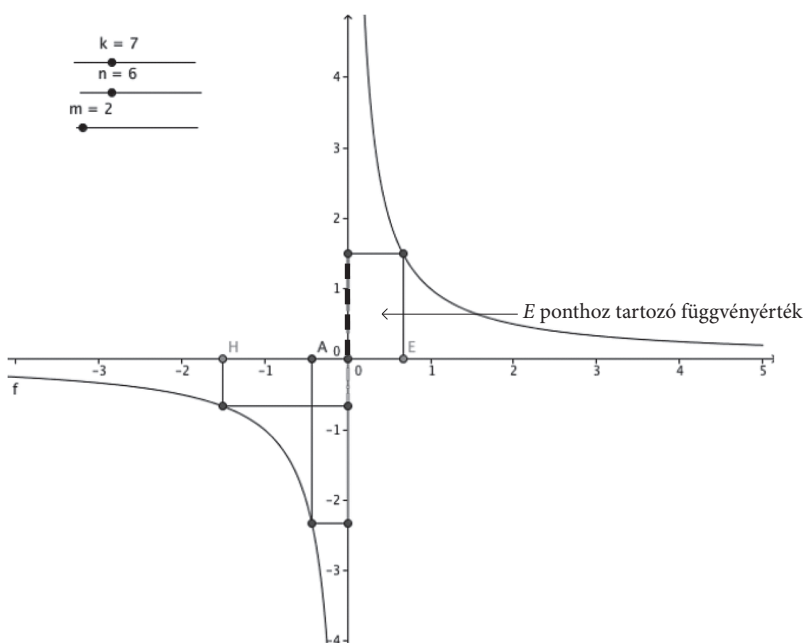
Ezen három példa mindegyike esetén a megfelelő függvényértékek sorozata végtelenbe tart.

A GeoGebrának köszönhetően a hallgatók saját maguk tapasztalhatják meg a fogalmat, hiszen saját maguk változtathatják a megfelelő pontok koordinátáit.

Nem szabad elfeledkeznünk arról, hogy a fogalomhoz ellenpéldát is mutassunk. Azaz vannak olyan függvények, amelyeknek nincs határértéke véges helyen. A következő példa segítségével erre szeretnénk a diákok figyelmét felhívni.

A legkézenfekvőbbnek az $R\setminus\{0\}\to R, x\mapsto 1/x$ függvény bizonyul. Nagyon sok helyen felhasználható függvény, már általános iskolában találkoznak vele a tanulók a fordított arányosság tanulása kapcsán.

6. ábra. Az $R\setminus\{0\}\to R, x\mapsto 1/x$ ***függvényhez tartozó ábra***



[7] Kovács J.–Takács G.–Takács M. (1998): *Analízis*. Budapest: Nemzeti Tankönyvkiadó.

Ebben az esetben az f:R\{0}→R, x↦1/x függvény 0-pontbeli határértékét vizsgáljuk. Megmutatjuk, hogy az *f* függvénynek $x_0 = 0$ pontban a jobb oldali határértéke plusz végtelen, míg a bal oldali határértéke mínusz végtelen. Ebből következik, hogy 0-ban nincs határértéke, mert a féloldali határértékek különbözőek.

A definícióhoz tartozó *5. ábrához* teljesen hasonló módon közelítjük meg a függvény értékeit az $x_0 = 0$ pont egy megfelelő környezetében.

Az *E* pont most is tart a 0-hoz, mert koordinátái (*4/n; 0*), s n növelésével a *4/n* tart 0-hoz. Ezáltal az *E* szigorúan monoton csökkenő módon tart 0-hoz. Az *E* ponthoz tartozó függvényértéket az *y*-tengelyen ismételten szaggatott vonallal jelöltük. Az *n* értékét szintén csúszkán tudjuk állítani. Az *n* növelésével a függvény értéke a plusz végtelenbe tart. A csúszkán történő mozgatással párhuzamosan látják a hallgatók a függvényértékek növekedését.

A *H* ponthoz tartozó értéket pontokkal szaggatott vonallal jelöltük. A csúszkával az m-et növelve tart a negatív végtelenbe a függvényérték.

Az *A* ponthoz tartozó függvényértéket pirossal jelöltük. A *k* csúszka állításával a pont hol negatív, hol pozitív értékek közt oszcillál, a $(-1)^n$ szorzónak köszönhetően. Ebben a konkrét példában nem csak az *A* pont ugrál a pozitív és a negatív értékek közt, hanem nagyon jól látszik, hogy a függvényértékek is hol pozitív, hol negatív értékeket vesznek fel, azaz nem tart sehova sem a függvényérték.

Természetesen az ábrák fejleszthetők, fejlesztendők. Az *5. ábra* esetén például nem célszerű mindhárom sorozatot egyszerre megmutatni, hiszen ekkor az ábra túlzsúfolt. Ajánlatosabbnak tartjuk az *5. ábrá*t három különböző ábraként kezelni, s csak az *5. és 6. ábrák* összehasonlítása esetén egyben. A színek helyes megválasztása is befolyásolja a felhasználhatóságot.

Ahhoz, hogy a hallgatók alkalmazni tudják ezeket az ábrákat a mindennapos tanulási folyamatban, egyrészt elérhetővé kell tenni számukra, másrészt különböző feladatokkal lehetővé kell tenni, hogy elegendő időt fordítsanak az ábrák tanulmányozására.

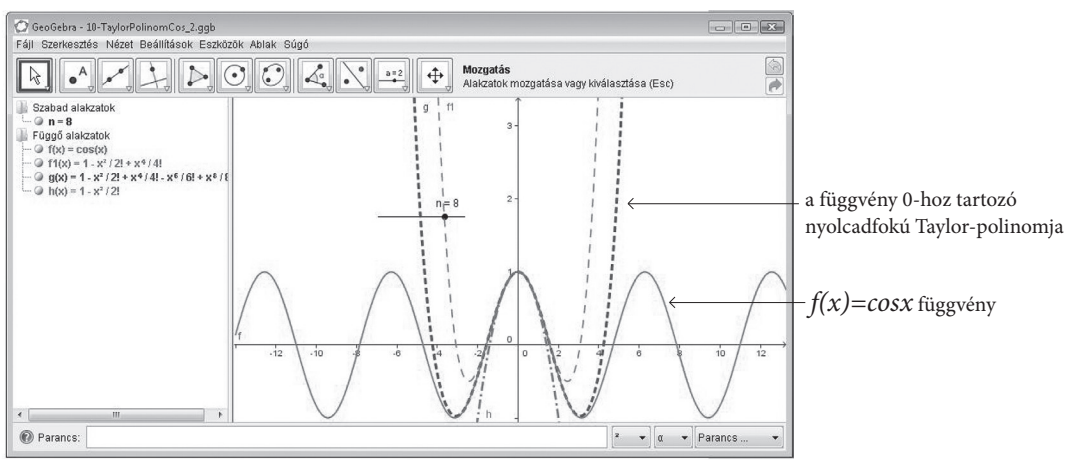
Taylor-polinom

A MacLaurin-sor, Taylor-sor és Taylor-polinom fogalmának ismertetésétől eltekintünk, az érdeklődő olvasónak javasoljuk [7] tanulmányozását.

A megértés kezdeti fázisában konkrét példákkal szemléltetjük a fogalmat. A *7. ábrán* folytonos vonallal az *f(x)=cosx* függvényt és sűrű szaggatott vonallal a függvény 0-hoz

tartozó nyolcadfokú Taylor-polinomját ábrázoltuk. Az *n* értéke csúszkával változtatható. A GeoGebra interaktivitását nagymértékben javítja a csúszkák alkalmazásának lehetősége. Csúszkával különböző paraméterek vizualizációját valósítjuk meg. A Taylor-polinom[cosx, 0, 8] paranccsal adható meg az *f(x)=cosx* függvény 0 középpontú nyolcadfokú Taylor-polinomja. A GeoGebra lehetőséget teremt arra, hogy az elkészített oktatási segédanyagunkat java appletként mentsük el, s tegyük elérhetővé a felhasználók számára. A *7. ábrán* bemutatott alkalmazáson megfigyelhető, hogy amint a Taylor-polinom fokszámát növeljük, annak grafikonja egyre jobban közelíti az *f(x)=cosx* függvény grafikonját. (Jelen alkalmazásban az *n* értéke 1 és 10 között változtatható.)

7. ábra. Függvény és Taylor-polinomja



Az ábrán jól látható, hogy a változtatható fokszámú polinomon kívül még két fix függvény is meg van adva (szaggatott, ill. pontozott vonallal). Ezek a másod- és negyedfokú Taylor-polinomok viszonyítási alapul szolgálnak a diákoknak.

[8] Murray, J. D. (2001): Mathematical Biology. Springer, *IAM*. Vol. 17.

[9] Simon, P. L.–Farkas, H. (1999): Wittmann, M., Constructing global bifurcation diagrams by the parametric representation method. *J. Comp. Appl. Math,* 108. Pp. 157–176.

Egy kémiai reakció modelljének matematikai vizsgálata

Ebben a fejezetben [8] alapján egy kémiai reakciót leíró kétváltozós differenciálegyenlet-rendszer nyereg-csomó bifurkációit vizsgáljuk. A vizsgálathoz a parametrikus reprezentáció módszerét (PRM) alkalmazzuk. Jelen dolgozatban a PRM-et nem részletezzük, az érdeklődő olvasó számára [9] szolgál részletes leírással.

Tekintsük [1] nyomán az alábbi differenciálegyenletet. Ebben a két reagens – X és Y – lineárisan bomlanak és az alábbiak szerint X aktiválja Y-t és Y aktiválja X-et.

$$\dot{x} = k_1 \frac{y^2}{K + y^2} - k_2 x \qquad (1)$$

$$\dot{y} = h_1 \frac{x^2}{H + y^2} - h_2 y \qquad (2)$$

ahol x és y rendre az X és Y reagensek koncentrációját jelöli, k_1, k_2, $h1$, h_2, K, H pozitív konstansok.

Írjuk fel az (1)-(2) rendszer egyensúlyi pontjait meghatározó egyenletrendszert:

$$0 = k_1 \frac{y^2}{K + y^2} - k_2 x \qquad (3)$$

$$0 = h_1 \frac{x^2}{H + y^2} - h_2 y \qquad (4)$$

A (4)-es egyenletből kifejezhető y az alábbiak szerint:

$$y = \frac{h_1 x^2}{h_2 (H + x^2)} \ . \qquad (5)$$

Ezt a (3)-ba behelyettesítve

$$\frac{k_1 h_1^2 x^4}{h_2^2 (H^2 + 2Hx^2 + x^4)} = k_2 x \left(K + \frac{h_1^2 x^4}{h_2^2 (H^2 + 2Hx^2 + x^4)} \right) \qquad (6)$$

adódik.

Legyenek a kontrollparaméterek k_1, és K, így az alábbiak szerint a diszkrimináns görbét a (k_1, K) paramétersíkban írjuk fel. Ezzel az (1)-(2) rendszer egyensúlyi pontjait meghatározó rendszer felírható

$$0=f_0+f_1 k_1+f_2 K=f(k_1,K,x) \text{ alakban.}$$

Itt $k_1=u_1$, $K=u_2$, $f_0=k_2 h_1^2 x^5$, $f_1=-h_1^2 x^4$, $f_2=h_2^2 k_2 x(H^2+2Hx^2+x^4)$.

A rendszer egyensúlyi pontjainak száma akkor változhat, ha $f(k_1, K, x)$ x-szerinti deriváltja szintén zérus, azaz $f'(k_1, K, x)=0$ teljesül.

Az $f=0$ és az $f'=0$ rendszerből:

$$k_1 = \frac{f_0 f_2' - f_2 f_0'}{f_2 f_1' - f_1 f_2'} \text{ és } K = \frac{f_1 f_0' - f_0 f_1'}{f_2 f_1' - f_2 f_2'}.$$

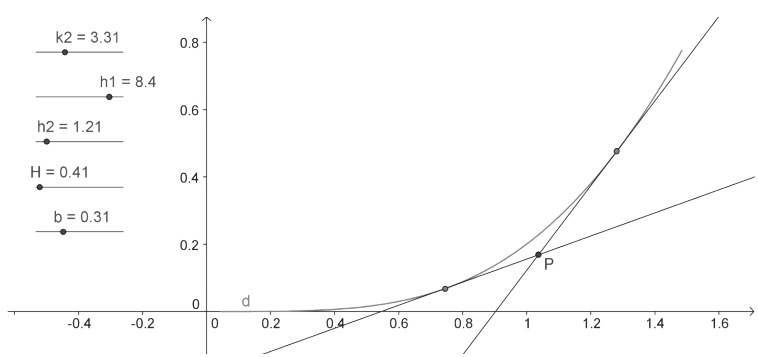
Tehát a (k_1, K) paramétersíkban ábrázoljuk a D-görbét x-szel paraméterezett görbeként. Itt a paraméter szó két különböző értelemben szerepel. A k_1 és a K paraméterek a rendszer paraméterei, míg a görbe paramétere a rendszer egyik állapotváltozója, x.

A görbe ábrázoláshoz a k_2, h_1, h_2 paramétereknek numerikus értéket kell adni. Tekintettel arra, hogy vizsgálatunk szempontjából a változó paraméterértékekhez tartozó bifurkációs görbe kvalitatív jellemzőinek változásai érdekesek, olyan eszközt keresünk az ábrázoláshoz, mellyel a paraméterek változtatása dinamikusan megjeleníthető. E célból tökéletes választás a GeoGebra.

Az alábbiakban az előző fejezetben meghatározott bifurkációs görbét a GeoGebra segítségével ábrázoljuk. A paraméterek értéke egy-egy csúszkán változtatható. b az intervallum felső határa, melyet szintén csúszkaként definiáltunk.

Az alábbi ábrán láthatjuk a paramétereket szemléltető csúszkákat, a D-görbét a paraméterek adott értéke mellett, valamint egy P, a görbén kívül eső pontot és az abból a görbéhez húzható érintőket.

8. ábra. Függvény és Taylor-polinomja



A következő tétel a PRM érintőtulajdonságának [9] egyszerű következménye:

Tétel: Az (1)-(2) rendszernek a paraméterek tetszőleges megválasztása esetén vagy pontosan nulla, vagy pontosan két megoldása van.

Összegzés

A dolgozat eredményei alapján megállapítható, hogy a GeoGebra az oktatásban és az alkalmazott kutatások támogatásában is megállja a helyét. Segítségével jól szemléltethetőek a tananyaghoz tartozó matematikai fogalmak és egyszerűbben, kevesebb energia befektetésével fogalmazhatóak meg sejtések, így a kutatók figyelmüket ezen sejtések bizonyítására fordíthatják.

[9] Simon, P. L.–Farkas, H. (1999): Wittmann, M., Constructing global bifurcation diagrams by the parametric representation method. *J. Comp. Appl. Math,* 108. Pp. 157–176.

LEITOLD FERENC *

Kártékony programkódok jellemzőiről

Összefoglalás: Ebben a cikkben egy olyan módszert mutatunk be, amely alkalmas arra, hogy a védelmi rendszerek felismerési képességeit felhasználva információt kaphassunk a programkódok kártékony tulajdonságára, a korára és az elterjedtségére vonatkozóan. Az eljárás lehetőséget ad arra, hogy utólagosan megítélhető legyen a teszteléshez használt kártékony programok halmaza, vagy esetleg ennek halmaznak a szűkítésével és a tesztelési eredmények ismételt összesítésével a tesztelés céljához jobban illeszkedő kártékony programhalmaz jöjjön létre.
Kulcsszavak: Kártékony kód; eljárás; tesztelés.

Abstract: In this article, we present a method that can be used to obtain information about the age and prevalence of malicious program codes using the recognition capabilities of protection systems. The procedure provides an opportunity to judge the set of malware used for testing in retrospect, or by narrowing this set and re-aggregating the test results to create a set of malware that is better suited to the purpose of testing.
Keywords: Malware; procedure; testing.

Bevezetés

A számítógépes hálózatokon keresztül történő, a számítógépek és a felhasználók kommunikációját kihasználó támadások, fenyegetések egyre nagyobb veszélyt jelentenek. [1], [2] Ide tartoznak az interneten terjedő kártevők [3], a célzott támadások, botnet-hálózatok igénybevételével vagy anélkül, és ide sorolhatjuk a social engineering-alapú, a személyes kommunikációra épülő támadásokat is. [4], [5], [6] Manapság a hálózati kapcsolaton keresztül tör-

*Dunaújvárosi Egyetem, Informatikai Intézet
E-mail: fleitold@uniduna.hu

[1] *Symantec Internet security threat report* (2019). https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

[2] Leitold, F. (2011): Testing protections against web threats Malicious and Unwanted Software (MALWARE), 6th International Conference on Malicious and Unwanted Software. Pp. 20–26.

[3] Tseng, C. H.–Wang S.–Wang, S-C.–Juang, T-Y. (2014): *Proactive malware collection and classification system: How to collect and classify useful malware samples?* International Conference on Information Science, Electronics and Electrical Engineering. Pp. 26–28.

téntő támadások azok, amelyek az informatikai támadások mintegy 95–97%-át jelentik. [7] Az elenyésző néhány százalékba tartozik többek között a cserélhető adathordozó (pl. pendrive) használata, illetve a fizikai károkozás is.

Programozott kártevők

A támadások célja, hogy a célba vett eszközt vagy felhasználót megpróbálja „átprogramozni", azaz elérni, hogy a támadó akaratát utasításait hajtsa végre. Ez lehet kizárólag social engineering-alapú, lehet teljesen technikai (felhasználói interaktivitást nem igénylő) és lehet social engineering módszereket is felvonultató, de alapvetően technikai. Amennyiben a technikai rész megjelenik, a támadások alapvetően valamilyen programozott kódra építenek. A legtöbb esetben a támadó célja, hogy ezt a (kártékony) programkódot az áldozat eszközére juttassa és ott ez a kód elinduljon. A kártékony programok definíció szerint olyan programkódok, amelyek képesek arra, hogy az eszköz (számítógép, okostelefon) felhasználójának tudta és beleegyezése nélkül valamilyen (általában kártékony) tevékenységet hajtsanak végre. Ilyen tevékenység lehet például: adatok törlése, titkosítása (ransomware), adatok továbbítása a támadó felé, e-mail-üzenetet továbbítása.

A támadások során használt kártékony programkódok köre folyamatosan növekszik, jelenleg 1 milliárd körül van a számuk. Ez nem azt jelenti, hogy ennyi kártékony programkód lenne, amik folyamatosan veszélyt jelentenek, csupán a töredékük az, amelyek potenciálisan veszélyes. Általában igaz, hogy egy kártékony programkód csupán néhány napig terjed.

Védelmi rendszerek

A védelmi rendszerek célja, hogy a támadónak a fenti tevékenységét megakadályozza, vagy úgy, hogy nem engedi, hogy a kártékony kód a felhasználó eszközét elérje (pl. firewall, e-mail-védelem), vagy úgy, hogy ha már elérte a felhasználó eszközét, akkor ott megakadályozza a kártékony kód végrehajtását (folyamatosan figyelő antivírus). Ebből az is látszik, hogy a védelmi rendszerek különböző típusú és módszerű eljárásokat használnak a felhasználók védelmében. Ez egyrészt különbséget jelent a „védelmi szituációban", azaz például egy firewall a hálózati forgalmat vizsgálja, egy antivírus az

[4] Chapman, M. T. (2015): *Advanced Persistent Testing: How to fight bad phishing with good.* PhishLine, http://www.phishline.com/advanced-persistent-testing-ebook

[5] Choo, K.-K. R. (2011): The cyber threat landscape: Challenges and future research directions. *Computers & Security.* 30. 8. Pp. 719–731. https://doi.org/10.1016/j.cose.2011.08.004

[6] Christodorescu, M.–Jha S.–Seshia S.–Song, D.–Bryant, R. (2005): *Semantics-Aware Malware Detection.* Proceedings – IEEE Symposium on Security and Privacy. Pp. 32–46. 10.1109/SP.2005.20.

[7] Burguera, I. –Zurutuza, U.–Nadjm-Tehrani, S.–Crowdroid (2011): *Behavior-Based Malware Detection System for Android.* SPSM '11. Pp. 15–26.

éppen elindítandó programkódot. Másrészt pedig az egyes védelmi rendszerek különböző algoritmusokat használnak a kártékony kód azonosítására (pl. bytesorozat-alapú keresés, ellenőrzőösszeg-alapú keresés, heurisztikus-keresés, viselkedésalapú-keresés, …). A védelmi rendszerek közös jellemzője, hogy valamilyen adatbázist használnak a működésük során, mely lehet egy (a gyártó által ismert kártékony programkódok segítségével) gépi tanulással előállított adatbázis, de lehet csak az ismert kártékony programkódok felismeréséhez szükséges adatbázis is. Egy védelmi rendszer szempontjából tehát vannak ismert és vannak ismeretlen kártékony programkódok. Ha megfelelőek egy védelmi rendszer algoritmusai és az adatbázisban szerepelnek az ismert kártékony programkódok adatai, akkor a védelmi rendszer ezeket képes felismerni (és azonosítani). Egy védelmi rendszer képessége esetén elsősorban az a kérdés, hogy mi a helyzet a (gyártó számára) ismeretlen kártékony programkódokkal. Képes-e arra, hogy ezeket valamilyen módon felismerje, illetve, ha nem, akkor mennyi időt vesz igénybe, mire a gyártó megfelelő frissítéseivel képes lesz felismerni? A védelmi rendszerek gyártóinak tehát folyamatos támogatást/szolgáltatást kell fenntartaniuk, hogy a védelmi rendszer megőrizze a hatékonyságát.

Threat Intelligence-szolgáltatások

A védelmi rendszerek fejlesztése, naprakészen tartása nem egyszerű feladat, azok a gyártók, akik sikeresen képesek a piacon jelen lenni, legalább néhány ezer főt foglalkoztatnak. Ugyanakkor a hatékony működés alapfeltétele, hogy ha valahol megjelenik egy új programozott kártevő, akkor arról mielőbb értesüljenek, illetve magát a kódot mielőbb megkapják, hogy elemzést követően az adatbázisukba építhessék. A védelmi rendszerek gyártói számára kézenfekvő a saját termékük használata, de rendelkeznek ettől független forrásokkal is. Ide sorolhatók a gyártók közötti, információ és threat-adatok cseréjére vonatkozó megállapodások, de ide tartoznak a védelmi rendszerek gyártóitól független threat-intelligence-szolgáltatók is. Ezek általában olyan szervezetek, akiknek az elsődleges feladata nem a védelmi rendszerek fejlesztése, hanem például internet-szolgáltatás és folyamatosan rendelkeznek a terjedő kártékony programkódokra vonatkozó adatokkal. Egy threat-intelligence-szolgáltatás többféle lehet. Vonatkozhat arra, hogy biztosítja az újonnan megjelenő kártékony programkódokat, vonatkozhat arra, hogy csak információt ad róluk, de előfordulhat olyan threat-intelligence-szolgáltatás is, amely egy adott kártékony programkód elemzését képes elvégezni. Egy kártékony programkódokat biztosító threat-intelligence-szolgáltatás esetén a rendszeresen elérhető újabb és újabb kártékony programkódokat *feed*nek nevezzük.

Védelmi rendszerek tesztelése

Amióta egy termék vonatkozásában a piacon alternatívák, választási lehetőségek jelentek meg, óhatatlanul előkerült a különböző képességek, tulajdonságok alapján történő összehasonlítás, illetve bizonyos standardeknek, minimumoknak való megfelelés vizsgálata. Nincs ez másként a védelmi rendszerek esetén sem. A vizsgálatok egyik iránya minden másfajta termékhez hasonlóan, a funkciók, beállítási lehetőségek, kezelhetőség stb. körére terjed ki. A védelmi rendszerek esetén viszont a kártékony kódok elleni védelmi képesség vizsgálata is felmerül. Mely kártékony programkódok esetén, milyen szituációkban alkalmas a védelemre, és milyen esetekben nem. 30 évvel ezelőtt ez egy egyszerű kérdés volt: az akkori DOS operációs rendszer alatt, az akkor létező 100-nál jóval kevesebb kártékony kód esetén egyszerűen el lehetett végezni egy vizsgálatot (még az akkor létező számítási kapacitást is figyelembe véve), ami minden lehetséges kártékony kódot számba vett és minden lehetséges szituációt felölelt. Manapság ez nem működik: 1 milliárdnál több kártékony kód létezik; az operációs rendszerek, bonyolult alkalmazások rengeteg beállítási lehetősége számtalan szituációt is jelent. A teljeskörű vizsgálat tehát nem működik. Ahhoz, hogy a védelmi képességre vonatkozó valamilyen vizsgálatot elvégezzünk, a kártékony kódok és a szituációk egy nagyon kis részhalmazával foglalkozhatunk csak. A cél persze az, hogy ezek a részhalmazok megfelelően mintázzák a vizsgálat célkitűzését. Ha egy vizsgálatnak az a célja, hogy a védelmek átlagos működése hogyan reagál a potenciális veszélyt jelentő kártékony kódokra (ami egy általános vizsgálat), akkor nyilván az aktuálisan terjedő kártékony kódok reprezentálására van szükség olyan szituációkban, amik a legáltalánosabbak. (De persze lehetnek ettől eltérő vizsgálatok is, például a zsarolóvírusokat milyen mértékben képesek a tűzfalak felismerni.) Manapság egy védelmi rendszer kártevő kódokkal szembeni vizsgálata nem reprodukálható, tekintettel elsősorban arra, hogy a védelmi rendszerek a gyártóik szervereinek szolgáltatását is igénybe veszik, amiknek a képessége folyamatosan változik.

A védelmi rendszerek gyártói és tesztelői 12 évvel ezelőtt megalapították az AMTSO (Anti-Malware Testing Standard Organization) szervezetet annak érdekében, hogy ajánlásokat, javaslatokat dolgozzanak ki annak érdekében, hogy a védelmi rendszerek vizsgálata korrekt és átlátható legyen.

A védelmi rendszerek vizsgálatánál, tesztelésénél az egyik legfontosabb kérdés, hogy milyen kártékony kódokat használjunk a teszteléshez. A tesztelőknek számos forrás (threat intelligence feed) áll a rendelkezésére, melyek lehetnek valamely védelmi rendszer gyártójához kötött, de lehet azoktól független is. Nyilván a független tesztelés érdekében a gyártókhoz kötött forrásokat célszerű megfelelő arányban használni. További probléma, hogy a vizsgálatot végzőknek biztosítani kell, hogy csak ténylegesen kártékony programkódokat használjanak, ismerniük kell, hogy az egyes kártékony kódok milyen régiek (mikor kezdődött el a terjedésük), illetve mennyire elterjedtek. Egy védelmi rendszereket tesztelő szervezet néhány tíz fős nagyságrendű mérete nem alkalmas arra, hogy kód-visszafejtéssel a kártékony tulajdonságról meggyőződjenek, valamint megfelelő információval sem rendelkeznek a terjedésekre vonatkozóan.

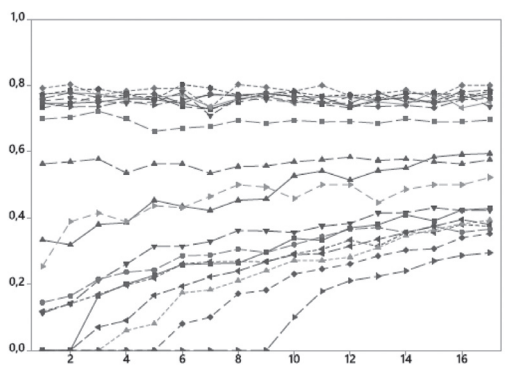
Az időablak-modell

Alábbiakban vázoljuk, hogy a védelmi rendszerek által szolgáltatott adatok alapján hogyan becsülhetők a kártékony kódok jellemzői [8]. Az *1. ábra* vízszintes tengelyén az idő (nap), függőleges tengelyén a kártékony kódok azonosításának aránya (azonosítás száma/vizsgálatok száma) látható. [9] Ezen tapasztalati adatsorra

$$y(t) = \alpha_1 \cdot \left(1 - \frac{1}{e^{\alpha_2(t-\alpha_3)}}\right) \qquad (1)$$

alakú függvényt illesztünk. Az (1) függvény paraméterei alapján becsülhető a kártevő programkód kora, terjedési sebessége és a fertőzési arány is. [10]

1. ábra. Kártékony kódok felismerésének aránya időben



Összegzés

Ebben a cikkben egy olyan módszert mutattunk be, amely alkalmas arra, hogy a védelmi rendszerek felismerési képességeit felhasználva információt kaphassunk a programkódok kártékony tulajdonságára, a korára és az elterjedtségére vonatkozóan. Az eljárás lehetőséget ad arra, hogy utólagosan megítélhető legyen a teszteléshez használt kártékony programok halmaza, vagy esetleg ezen halmaz szűkítésével és a tesztelési eredmények ismételt összesítésével a tesztelés céljához jobban illeszkedő kártékony programhalmaz jöjjön létre.

[8] Bognár, L.–Joós, A–Nagy, B. (2018): An Improvement for a Mathematical Model for Distributed Vulnerability Assessment *Acta Universitatis Sapientiae Mathematica.* 10. (2.) Pp. 203–217.

[9] Bognár, L.–Joós, A.–Nagy, B. (2020): Assessing the effect size of users' consciousness for computer networks vulnerability. *Acta Universitatis Sapientiae Mathematica.* 12. (1.) Pp. 14–29.

[10] Joós, A.–Bognár, L.–Nagy, B. (2020): Time Evolution Model for Classifying Files in Antivirus Testing Procedures. In: *The 1st Conference on Information Technology and Data Science: Book of abstract.* Pp. 45–47.

KOCSÓ EDINA *–CSERNÉ PEKKEL MÁRTA **–FAUSZT TIBOR ***–BOGNÁR LÁSZLÓ ****

Matematika kurzusok a hallgatói vélemények tükrében

Összefoglalás: Jelen dolgozatban a Dunaújvárosi Egyetem matematika kurzusait vizsgáljuk a hallgatók szemszögéből. Néhány kurzus esetén kérdőíves felmérést végeztünk. Ezek eredményei alapján a kurzusok további fejlesztése szempontjából vonunk le következtetéseket.
Kulcsszavak: Matematikaoktatás; egyetem; hallgatói vélemények.

Abstract: In this work we examine the mathematics courses of the University of Dunaújváros from the students' point of view. For some courses, we conducted a questionnaire survey. Based on these results, we draw conclusions for the further development of the courses.
Keywords: Mathematics education; university; student opinions.

Bevezetés

A Dunaújvárosi Egyetem hallgatói több képzési szinten, rendkívül nagy arányban hallgatnak matematikát. Az őszi félévben Matematika 1 és Matematika 3 tantárgyak szerepelnek a tantervben. A tantárgyak elsajátítását az elmúlt évek digitális átalakulásának megfelelően [1], [2] a tanórai jegyzetek, a kötelező- és ajánlott irodalmak mellett az egyes témakörökhöz tematikusan összeállított videóanyagok, gyakorló feladatsorok, önellenőrző tesztek segítik, melyek minden hallgató számára elérhetőek a Moodle-rendszeren keresztül, valamint rendszeres online Microsoft Teams felületen tartott konzultációk támogatják a tantárgy sikeres teljesítését.

A Moodle-rendszer az interaktív tanulás elősegítésére sokféle funkciót kínál a hallgatók számára. A Moodle nagy előnye, hogy lehetőséget biztosít a tanítási-tanulási folyamat három résztvevője (tanuló–tanár–tananyag)

*Dunaújvárosi Egyetem, Tanárképző Központ
Email: kocsoe@uniduna.hu

**Dunaújvárosi Egyetem, Tanárképző Központ
Email: csernepm@uniduna.hu

***Dunaújvárosi Egyetem, Informatikai Intézet
Email: fausztt@uniduna.hu

****Dunaújvárosi Egyetem, Informatikai Intézet
Email: bognarl@uniduna.hu

[1] Benedek A. (Szerk.) (2008): *Digitális pedagógia.* Budapest: Typotex.

[2] Racsko, R. (2017): *Digital Transformation in Education. (Digitális átállás az oktatásban)* Veszprém: School Culture Books (Iskolakultúra-könyvek). P. 52.

[3] Váraljai, M.–Nagy, B. (2019): A Survey in Issues of Disruptive Technologies to Broaden Learning for The Future Students. In: Baranyi, Péter (Eds.): Proceedings of the 10th IEEE International Conference on Cognitive Infocommunications: CogInfoCom 2019 Piscataway (NJ), Amerikai Egyesült Államok: IEEE. Pp. 391–396.

[4] Molnár, Gy.–Szűts Z.–Biró, K. (2018): Use of Augmented Reality in Learning. *Acta Polytechnica Hungarica.* 15. (5.) Pp. 209–222.

[5] Szabó, Cs. M.–Bartal, O.–Nagy, B. (2020): The Methods and IT-tools Used in Higher Education Assessed in the Characteristics and Attitude of Gen Z. *Acta Polytechnica Hungarica.* Megjelenés alatt.

[6] Kővári, A. (2019.): Adult education 4.0 and Industry 4.0 challenges in lifelong learning. *Pedacta.* 9. (1.) Pp. 9–16.

[7] Chmielewska, K.–Gilányi, A. (2018): Educational Context of Mathability. *Acta Polytechnica Hungarica.* 15. (5.) Pp. 223–237.

[8] Kővári, A.–Rajcsányi-Molnár, M. (2020): Mathability and Creative Problem Solving in the MaTech Math Competition. *Acta Polytechnica Hungarica.* 17. (2.) Pp. 147–161.

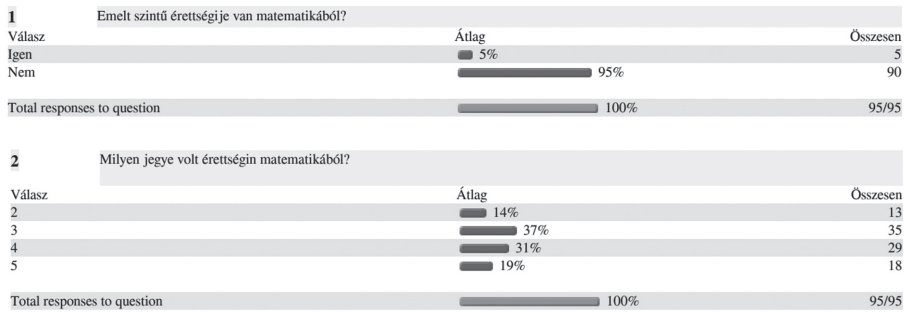
[9] Bacsa-Bán, A.–Marcinkevičienė, V. (2016): Comparison of studies‘ termination reasons in College of Dunaujvaros (Hungary) and Kauna Kolegija/University of Applied Sciences Faculty of Technologies and Landscaping (Lithuania). In: Maior, Enikő–Tóth, Péter–Varga, Anikó (Szerk.): *Empirikus kutatások az oktatásban határon innen és túl.* Budapest: Óbudai Egyetem, Trefort Ágoston Mérnökpedagógiai Központ. Pp. 272–296.

számára, hogy időtől és helytől függetlenül találkozzon. A hallgatók az oktató által feltöltött polimédia-anyagokat, videó leckéket számtalanszor megnézhetik, elolvashatják az elméleti összefoglalókat, feladatokat oldhatnak meg, kérdésbankból generált kérdések/tesztek segítségével ellenőrizhetik tudásukat, fórumon keresztül kommunikálhatnak diáktársaikkal és tanáraikkal, számonkérés is lebonyolítható a beépített tesztek segítségével, valamint lehetőség van a hallgatók értékelésére és az aktivitásuk követésére. [3], [4] A tanulási útmutatásokkal támogatott jól felépített és átgondolt tananyagok lehetővé teszik az önálló tanulást is. [5], [6] A félév során a tananyagok további tökéletesítése céljából – hasonlóan más felmérésekhez [3] – mindkét tárgy esetén kérdőíves felmérést végeztünk a hallgatók körében. A felmérés célja, hogy a kurzusok megfelelő fejlesztésével támogassuk a hallgatók matematikai készségeinek, képességeinek fejlesztését [7], [8], továbbá növeljük a hallgatók sikerességét. [9]

Matematika 1.

A *Matematika 1.* tantárgy az alapképzési szakokon az őszi félévben szerepel. Jellemző átadási mód a heti 3 óra tantermi gyakorlat. A tantárgy elsődleges képzési célja, hogy a hallgatók további tanulmányaikhoz a nélkülözhetetlen matematikai alapokat megszerezzék. A tantárgyat tanuló hallgatók többsége számára ez az első félév az egyetemen, így a korábbi tanulmányok vizsgálata során az érettségiről kérdeztük őket. Majdnem mindegyik hallgató középszintű matematika érettségivel jön a középiskolából, csak 5% tett emelt érettségit matematikából. A hallgatók kevesebb, mint 20%-a hoz jeles matematika érettségit, azonban az elégséges érdemjegy aránya is meglehetősen magas, 14%.

1. ábra. Matematika 1 kurzust teljesítő hallgatók érettségi eredménye matematika tantárgyból



1 Emelt szintű érettségije van matematikából?

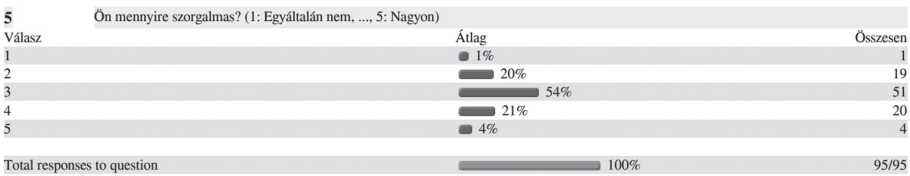
Válasz	Átlag	Összesen
Igen	5%	5
Nem	95%	90
Total responses to question	100%	95/95

2 Milyen jegye volt érettségin matematikából?

Válasz	Átlag	Összesen
2	14%	13
3	37%	35
4	31%	29
5	19%	18
Total responses to question	100%	95/95

A hallgatók 55%-a gimnáziumban, 45%-a más középiskolában végezte középfokú tanulmányait. Saját megítélése szerint a hallgatók 54%-a közepesen szorgalmas, míg az egyéb kategóriák normális eloszlásra hasonlító arányban találhatók a válaszok között.

2. ábra. A hallgatók szorgalma saját megítélésük szerint

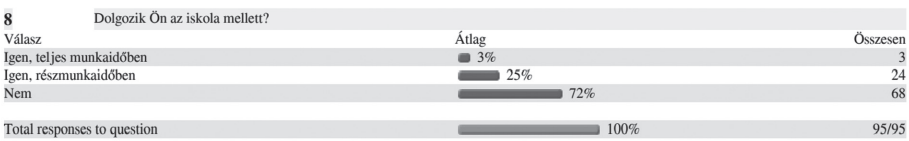


5 Ön mennyire szorgalmas? (1: Egyáltalán nem, ..., 5: Nagyon)

Válasz	Átlag	Összesen
1	1%	1
2	20%	19
3	54%	51
4	21%	20
5	4%	4
Total responses to question	100%	95/95

A hallgatók iskolai teljesítményét az is befolyásolja, hogy energiájukat milyen mértékben tudják a tanulásra fordítani. Jelen kérdőívet kitöltő hallgatók több mint negyede dolgozik az iskola mellett.

3. ábra. Munkahelyi elfoglaltságok a hallgatók körében



8 Dolgozik Ön az iskola mellett?

Válasz	Átlag	Összesen
Igen, teljes munkaidőben	3%	3
Igen, részmunkaidőben	25%	24
Nem	72%	68
Total responses to question	100%	95/95

A hallgatók korábbi tapasztalata szerint a különböző tananyagtípusok különböző módon segítik őket a tananyag megértésében. A következő kérdés (Melyik tananyagtípus(ok) segíti(k) Önt a legjobban a matematika vizsgára való felkészülésben? Jelöljön be maximum hármat!) arra keresi a választ, hogy melyik típust találják a leghasznosabbnak. Jól látható, hogy a különböző oktatóvideók hasznosulnak legjobban (akár a Moodle-rendszerben elérhető professzionális polimédia tananyagokra, akár az élő kontakt órákat leginkább megidéző, Microsoft Teams felületen tartott tanórákról készült videókat tekintjük. Érdekes, hogy a nyomtatott tananyagokat a hallgatók mindössze 6%-a használja. Elgondolkodtató – és mindenképpen megoldandó problémát takar –, hogy a hallgatók 34%-a saját maga próbál az interneten tananyagokat felkutatni.

4. ábra. Tananyagtípusok hasznossága a hallgatók szerint

9

Válasz	Átlag	Összesen
a Moodle videók	66%	62
a Moodle videók után kitűzött tesztek	37%	35
a Moodle fejezet végén található témazáró tesztek	26%	24
a Teamsen megtartott órák, illetve az azokról készült videók	78%	73
a Kovács J.-Takács M.-Takács G.: Analízis tankönyv ("fekete biblia")	5%	5
a nyomtatott Analízis példatár	1%	1
az interneten talált tananyagok	34%	32
Total responses to question	99%	94/95

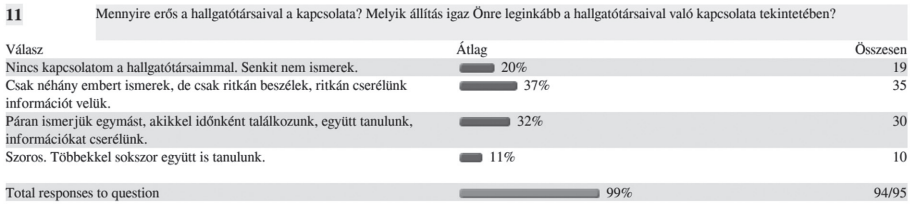
A 2020/21. tanév őszi félévében rendhagyó módon, online történt a matematika kurzusok oktatása. A kurzusok monitorozása szempontjából fontos kérdés, hogy a hallgatók a tananyagokat online érik el vagy letöltik a számítógépükre, s offline használják ezeket.

5. ábra. A tananyagok elérési módjának eloszlása

10 Hogyan használja a fenti tananyagokat?

Válasz	Átlag	Összesen
Mindig online, a neten használom.	31%	29
Letöltöm a gépemre, és offline használom.	3%	3
Változó. Online és offline is használom.	66%	62

6. ábra. Hallgatói kapcsolatok erőssége



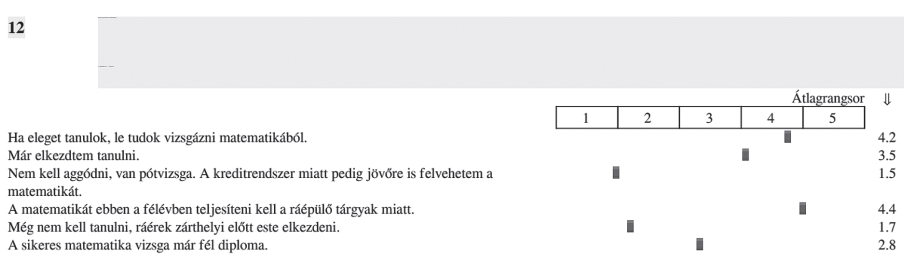
11 Mennyire erős a hallgatótársaival a kapcsolata? Melyik állítás igaz Önre leginkább a hallgatótársaival való kapcsolata tekintetében?

Válasz	Átlag	Összesen
Nincs kapcsolatom a hallgatótársaimmal. Senkit nem ismerek.	20%	19
Csak néhány embert ismerek, de csak ritkán beszélek, ritkán cserélünk információt velük.	37%	35
Páran ismerjük egymást, akikkel időnként találkozunk, együtt tanulunk, információkat cserélünk.	32%	30
Szoros. Többekkel sokszor együtt is tanulunk.	11%	10
Total responses to question	99%	94/95

A hallgatók tanulmányai során mutatott teljesítményét befolyásolja, hogy társaival milyen a kapcsolatuk. A képzés megkezdésekor nyilván ezek a kapcsolatok még gyengék. Ettől függetlenül már az első félévben a hallgatók 11%-a szerint szoros a kapcsolata a többi hallgatóval. Ez vélhetően korábban meglevő kapcsolatokon alapul: elképzelhető, hogy többen jöttek azonos középiskolából, vagy ugyanarról a lakóhelyről. Sajnos az online oktatás ezen kapcsolatok erősödését nem könnyíti meg. A további félévek során erre is érdemes figyelmet fordítani a kurzusok tervezése során.

Az utolsó kérdésben arra kerestük a választ, a hallgatók mennyire érzik fontosnak, hogy ebben a félévben teljesítsék a *Matematika 1.* tantárgyat. A tanulmányi előrehaladásuk szempontjából ez nyilvánvalóan meghatározó, hiszen erre a tárgyra sok további tantárgy épül, melyeket nem tudnak felvenni, amíg a Matematika 1. tárgyat nem teljesítik. A kapott válaszok alapján megállapítható, hogy a hallgatók érzik ennek a tárgynak a súlyát, s ennek megfelelően tanulnak.

7. ábra. A „Mennyire igazak Önre az alábbi állítások? (1: Egyáltalán nem., ..., 5: Teljesen.)" kérdésre adott válaszok



12

	Átlagrangsor ⇓	1	2	3	4	5	
Ha eleget tanulok, le tudok vizsgázni matematikából.							4.2
Már elkezdtem tanulni.							3.5
Nem kell aggódni, van pótvizsga. A kreditrendszer miatt pedig jövőre is felvehetem a matematikát.							1.5
A matematikát ebben a félévben teljesíteni kell a ráépülő tárgyak miatt.							4.4
Még nem kell tanulni, ráérek zárthelyi előtt este elkezdeni.							1.7
A sikeres matematika vizsga már fél diploma.							2.8

[10] Erdélyi, K. (2012): How Information Technology Helps to Mitigate Difficulties. Occurred In: Teaching Intercultural Groups, ICETA 2012 10th IEEE International Conference on Emerging eLearning Technologies and Applications, Stará Lesná, November 8–9. P. 97.

[11] Nagy B. (2018): VR alkalmazásának lehetősége a matematika oktatásában. In: Baranyiné Kóczy Judit–Fehér, Ágota (Szerk.): XXI. Apáczai-napok konferencia. *„Útkeresés és újratervezés"*. Tanulmánykötet. Győr: Széchenyi István Egyetem, Apáczai Csere János Kar. Pp. 305–309.

[12] Ujbányi, T.–Stankov, G.–Nagy, B. (2019a): A transparent working environment in MaxWhere virtual space. In: Baranyi, Péter (Ed.): *Proceedings of the 10th IEEE International Conference on Cognitive Infocommunications: CogInfoCom 2019*. Piscataway (NJ): IEEE. Pp. 475–478.

[13] Ujbányi, T.–Stankov, G.–Nagy, B. (2019b): Eye tracking based usability evaluation of the MaxWhere virtual space in a search task. In: Baranyi, Péter (Ed.): *Proceedings of the 10th IEEE International Conference on Cognitive Infocommunications: CogInfoCom 2019*. Piscataway (NJ): IEEE. Pp. 469–474.

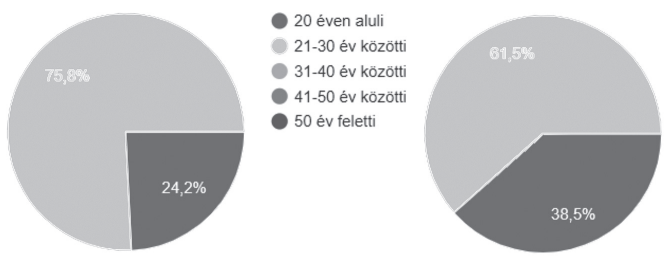
Matematika 3.

A *Matematika 3*. tantárgy az alapképzési szakokon szintén az őszi félévben szerepel. Jellemző átadási mód a heti 3 óra tantermi gyakorlat.

A tantárgy elsődleges képzési célja, hogy a hallgatók a szakterületüknek megfelelő matematikai feladatok megoldásához szükséges módszereket, eljárásokat ismerjék és alkalmazni is tudják.

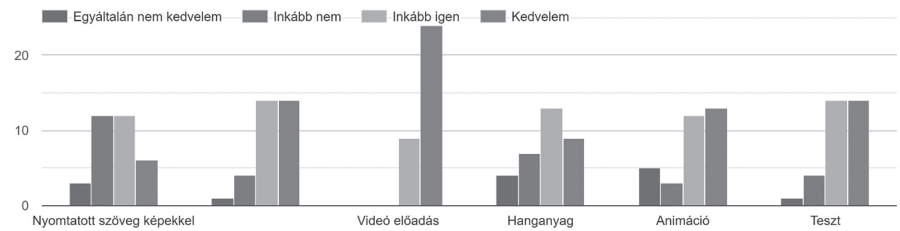
Jelen dolgozatban a magyar és az angol nyelvű nappali tagozatos *Matematika 3.* kurzus hallgatói által kitöltött felmérés néhány kérdését mutatjuk be. Az angol nyelvű képzések sok esetben más képet mutatnak. [10]

8. ábra. A Matematika 3. nappalis kurzusok hallgatóinak életkora (balra a magyar nyelvű kurzus, jobbra az angol nyelvű kurzus)

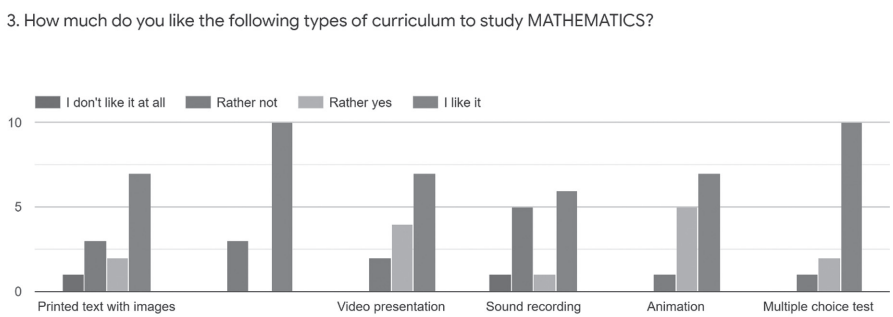


A *9. és a 10. ábrán* a hallgatók által kedvelt tananyagtípusokat láthatjuk. A magyar nyelvű képzés hallgatói körében kiemelkedik a videóelőadások aránya, míg az angol nyelvű kurzus esetén a feleletválasztásos tesztek és az elektronikus szöveg aránya magas. Ezen tananyagelemek már most is megtalálhatók a rendszerben. [11], [12], [13]

9. ábra. Tananyagtípusok elfogadása a magyar nyelvű Matematika 3. kurzus esetében



10. ábra. Tananyagtípusok elfogadása az angol nyelvű Matematika 3. kurzus esetében

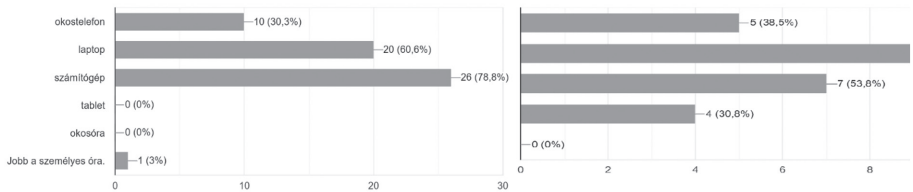


A tanuláshoz a hallgatók jobbára laptopot vagy asztali számítógépet használnak. Nem meglepő, hogy a matematikai tanulmányaikhoz nem használják az okosórákat. (Bár bizonyos felhasználási módok elvileg lehetővé tennék.) Okostelefonokat a hallgatók 30–40 %-a használ az egyes kurzusokon, így a tananyagokat ezen eszközökre is érdemes fejleszteni. [14], [15]

[14] Sík D.–Molnár Gy. (2019). Élményalapú, okostelefonnal támogatott atipikus oktatásmódszertani megoldások a nyitott tananyagfejlesztés kiterjesztésére. *Opus et Educatio.* 6. (2.).

[15] Orosz, B.–Kovács, C.–Karuovic, D.–Molnár, Gy.–Major, L.–Vass, V.–Zoltán, Sz.–Námesztovszki, Zs. (2019). Digital education in digital cooperative environments. Journal of Applied Technical and Educational Sciences. 9. (4.) Pp. 55–69.

11. ábra. A tanulás során használt digitális eszközök a magyar (balra) és az angol (jobbra) nyelvű kurzusok esetén



Mindkét hallgatói csoport az online kurzusok erősségeként értékeli, hogy nem kell utazással időt tölteni és a tanulásra fordított időt teljes mértékben ők határozhatják meg.

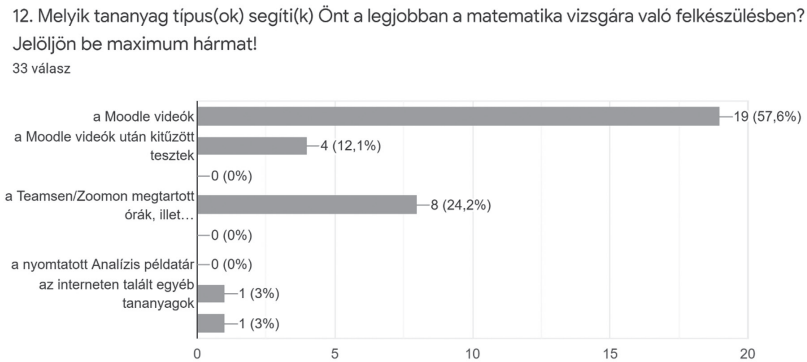
Legnagyobb hátrányként ugyanúgy azt élik meg, hogy több a kijelző előtt eltöltött idő és kevesebb a személyes kapcsolat a hallgatótársakkal. A tantárgy nehézségének megítélése a két csoport esetében különböző.

Míg a magyar hallgatók több, mint fele szerint 4–6 óra szükséges hetente a tárgy sikeres elvégzéséhez, addig ugyanígy az angol nyelvű csoport mintegy 15%-a gondolja.

12. ábra. A Matematika 3. tanulására fordított idő a magyar (balra) és az angol nyelvű (jobbra) kurzus esetében

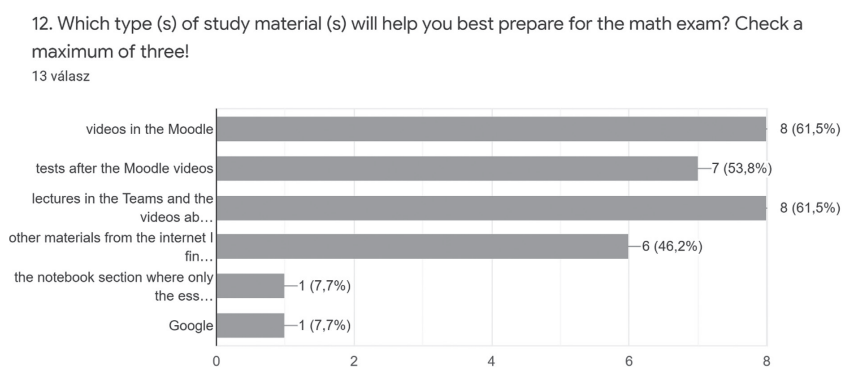
A felhasznált tananyagtípusok a *Matematika 3.* kurzus esetén eltérést mutatnak a magyar és angol nyelvű kurzus esetében.

13. ábra. A magyar nyelvű hallgatók által kedvelt tananyagtípusok



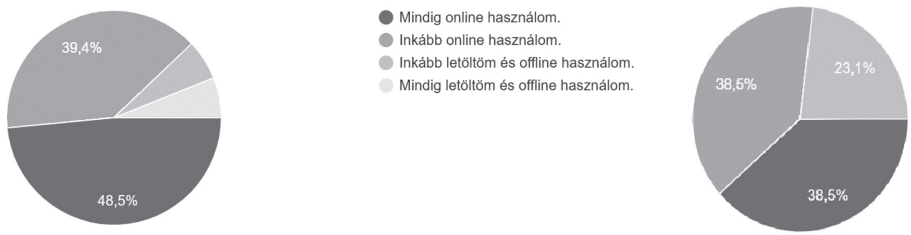
A *13. ábra* alapján a magyar nyelvű hallgatók mintegy 58%-a szerint a leghasznosabbak a Moodle-rendszerben elérhető videók, s az élő órákról készült felvételek a Teamsen csak 24% szerint hasznosak. A *14. ábra* alapján az angol nyelvű kurzusok esetén a Teamsen rögzített órák és a Moodle-rendszerben elérhető videók mindegyike a hallgatók több, mint 61 %-a szerint hasznosak.

14. ábra. Az angol nyelvű hallgatók által kedvelt tananyagtípusok



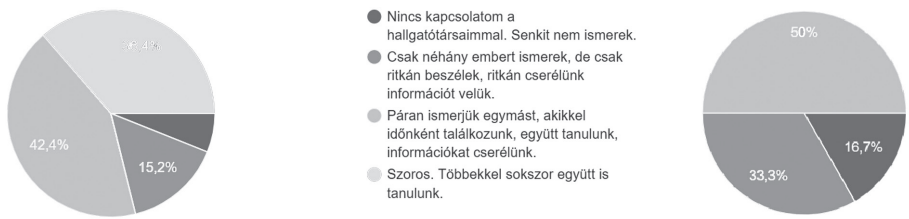
A *15. ábrán* a tananyagok elérési módja látható. A magyar nyelvű hallgatók között még előfordul, hogy letölti és offline használja a tananyagokat. Látható ugyanakkor, hogy az online elérés mindkét csoport esetén túlsúlyban van.

15. ábra. A tananyagok elérése a magyar nyelvű (balra) és az angol nyelvű kurzus (jobbra) esetén



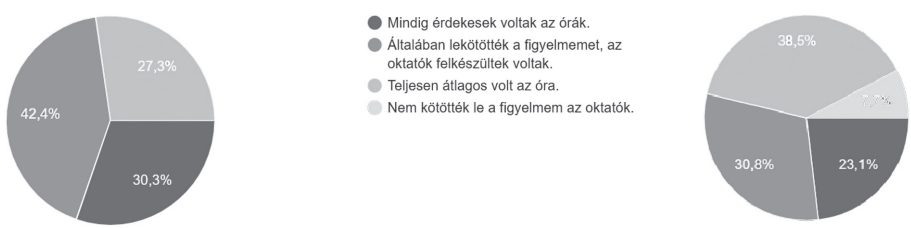
A *16. ábra* a hallgatók társas kapcsolatait mutatja be. Jól látható, hogy a Matematika 1. kurzus hallgatóihoz képest a magyar nyelvű *Matematika 3.* kurzus hallgatóinak mennyivel több a kapcsolata a társaikkal. Sajnos az is látható, hogy az angol nyelvű kurzusok esetén ilyen sok szoros kapcsolat nem alakult ki.

16. ábra. A magyar és angol nyelvű kurzusok hallgatóinak kapcsolata a hallgatótársakkal



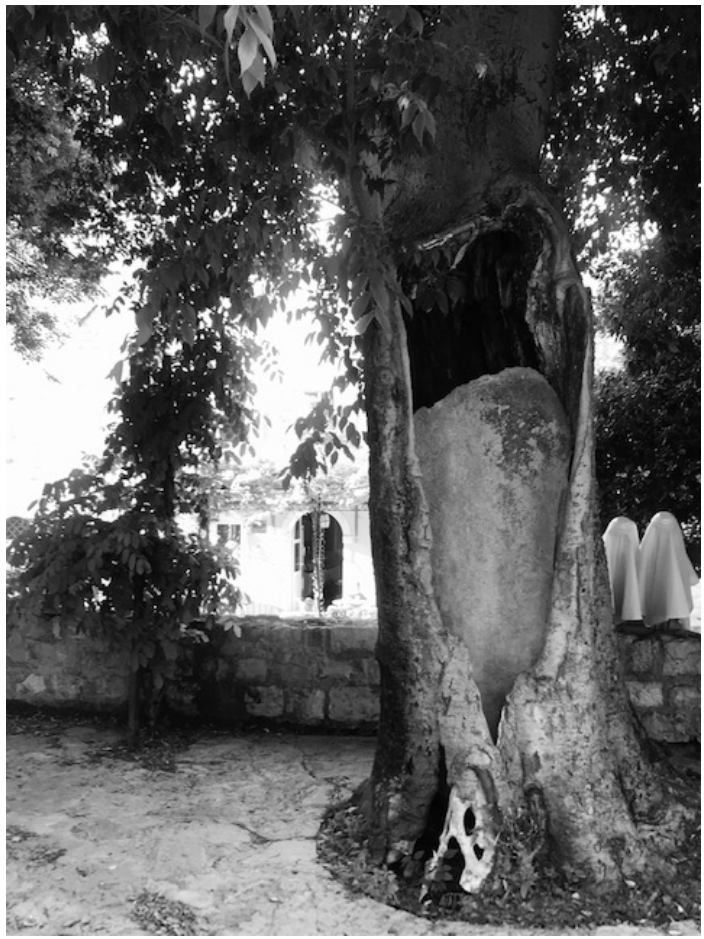
A *17. ábrán* azt vizsgáltuk, mennyire voltak elégedettek a hallgatók a Matematika 3 órákkal.

17. ábra. „Elégedett volt az oktatók előadásaival?" kérdésre adott válaszok



Összegzés

A dolgozatban a Dunaújvárosi Egyetem matematika kurzusait vizsgáltuk a hallgatók szemszögéből. Néhány kurzus esetén végzett kérdőíves felmérés eredményei alapján a kurzusok további fejlesztése szempontjából vontunk le következtetéseket. Ezek alapján a kurzusokon alkalmazott tananyagok megfelelő módosításával célunk a hallgatói megelégedés fokozása.



KRISZTINA GYŐRFFYNÉ HOLLÓ *

The Human Factors of the IT Risk Management

Abstract: Nowadays the informatics and so its IT devices, IT services become increasingly important. Ongoing digital transformation impacts many parts of our daily life, from the ever-increasing integration of digital technologies in all sectors of the economy to the societal impact of emerging technologies such as Artificial Intelligence (AI). Information highways, the exponentially developing IT devices, and applications provide an opportunity to obtain and utilize extraordinary and rich information. At the same time, the risks are less dealt with, which are netting the IT tools. Information security risks are always affecting IT systems. The based on conclusions of the carried-out measurement and research in the topic of the public servant and education, it can be considered at least three base factors or group in the building IT security systems. These base factors or groups are part of the information security systems. Specifically, these are the user's behaviour, the protected IT system, and malicious activity. Each significant component influences the design, construction, and use of the IT system. The focus of investigates is the components of the IT security management system, but especially the human factor and the damage. By applying the math and education method, IT engineers can be able to realize a higher IT protection level.

The relevant part of the research is the IT risk analysis and treatment, analysis of the human weakest links, and need for digital competence development in education. In this case, the human factor, the development of IT security awareness, and the extent of the caused damage are investigated.

Keywords: Information security; management; cybercrime; factor; human; damage; IT security awareness.

* *National University of Public Service Budapest, Hungary University of Pannonia Veszprém*
E-mail: gyorffy.kriszta@gmail.com

Összefoglalás:
Napjainkban az informatika, az informatikai eszközök és szolgáltatások egyre fontosabbá válnak. A digitális átalakulás, a feltörekvő technológia, úgymint a mesterséges intelligencia (AI) a mindennapi életünk számos részét érinti, a gazdaság minden ágazatát és a társadalmunkat egyaránt. Az információs autópályák, az exponenciálisan fejlődő informatikai eszközök és alkalmazások lehetőséget nyújtanak a rendkívüli és gazdag információk megszerzésére és felhasználására. Ugyanakkor a kockázatok kezelését, amelyek hatással vannak az informatikai eszközökre, már elhanyagolják. Az információbiztonsági kockázatok mindig befolyásolják az informatikai rendszerek működését. Az elsődlegesen közszolgálati és az oktatási szférában végzett mérés és kutatás következtetései alapján az informatikai biztonsági rendszerek felépítésében legalább három tényező figyelhető meg.
Az alaptényezők az információbiztonsági rendszerek részét képezik, amelyek a felhasználó viselkedése, a védett informatikai rendszer és a rosszindulatú tevékenységek témái köré csoportosulnak. A csoportok jelentősen befolyásolják az informatikai rendszer tervezését, felépítését és használatát. Ezúttal a vizsgálatok középpontjában az informatikai biztonsági menedzsment rendszer összetevői állnak, de különösen az emberi tényező és a veszteségek.
A matematikai és tudatosítási módszer alkalmazásával az informatikai mérnökök magasabb IT védelmi szintet tudnak megvalósítani. A kutatás releváns része az informatikai kockázatelemzés és -kezelés, az leggyengébb láncszem elemzése, valamint a digitális kompetencia fejlesztésének igénye. Ebben a tanulmányban az emberi tényezőt, az informatikai biztonságtudatosság jelentőségét és az információbiztonsági kár mértékét vizsgálom.
Kulcsszavak: Információbiztonság; menedzsment; számítógépes bűnözés; faktor; emberi; kár; informatikai biztonságtudatosság.

Introduction

Cyber threats and attacks are becoming more common, sophisticated and damaging. In the last years the NATO cyber defence centre [1], the International Telecommunication Union (ITU) [2] and the European Union Agency for Network and Information Security (ENISA) [3] , so this institutes have drawn attention to recommendations, strategies and directives at various levels of organization that minimum conditions and measures are indispensable to hold cyberspace safe at a minimum level.

Digital competence development started well before the COVID-19 crisis, and evidence was clear on the need to support the digital competence development of adults and young people in Europe. Today more than ever, being digitally competent is both a necessity and a right. However, digital skills levels across Europe remain unsatisfactorily low, with 44% of EU citizens having an insufficient level of digital skills. In addition, digital divides related to gender, socio-economic background and urban/rural areas persist. Cyberspace defence is very important and it is not only concerning the national security, but it affects the economy, the society, the members of the information technology and communication networks, such as an international, a state, or a civilian participator. Therefore, in an individual case, it may become a potential target or victim. The best way to stop cybercrime is to prevent it from happening in the first place. It is part of that, the public, so citizens and businesses need to be provided with accurate, relevant information on how to keep themselves safe online and to secure their devices and data.

Generally, the government is strongly supportive of growing the use of the Internet and recognizes the need to provide adequate and accurate information on the risks to consumers should they decide to use internet services. The primary purpose of any of our safety information is to ensure that the public and business has accurate information to help them protect themselves. The influencing factors of the cybersecurity risk management usually are relevant, so it has to be mentioned such as the European regulations, some informative and awareness events, and data as well as some general prevention opportunities and some factors of information security risk, so the human factors and the social engineering risk. By the presented math research, a quantitative approach (statistical analysis) is adopted to provide an approach to quantify the potential cybersecurity capability aptitudes of indus-

[1] *National Cyber Security Strategy Guidelines.* https://ccdcoe.org/library/publications/national-cyber-security-strategy-guidelines, download: December 4, 2020

[2] Understanding cybercrime: Phenomena, challenges and legal response, International Telecommunication Union, Geneva, Switzerland, 2012

[3] *Governance framework for European standardization.* https://www.enisa.europa.eu/publications/policy-industry-research, download: December 4, 2020

trial human actors, identify the least security-capable workforce in the operational domain with the greatest susceptibility likelihood to cyber-attacks (weakest link) and guide the enhancement of security assurance. To support these objectives, a Human-factored

Cyber Security Capability Evaluation approach is presented using conceptual analysis techniques. The method is part of risk management which can be applied in education, industry, aeronautics, and many areas of information technology. So the application of the method needs to be incorporated into both education and practical implementation.

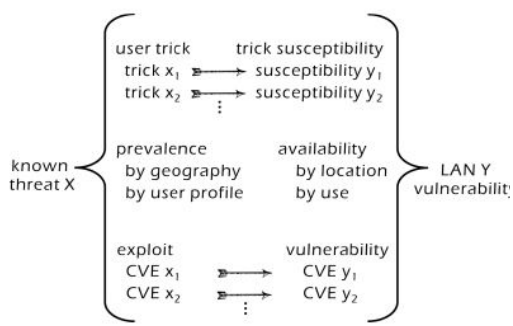
The research is related to the project of the University of Dunaújváros EFOP-3.6.1-16-2016-00003 "Long-term strengthening of R&D&I processes at the University of Dunaújváros" to the work of the research group "Man-computer interface based on manual gesture control".

The factors of the cybercrimes

The factors of the cyber-threats

The protected IT system can be investigated by mathematical algorithms, which is presented in the *figure 1 and 2*.

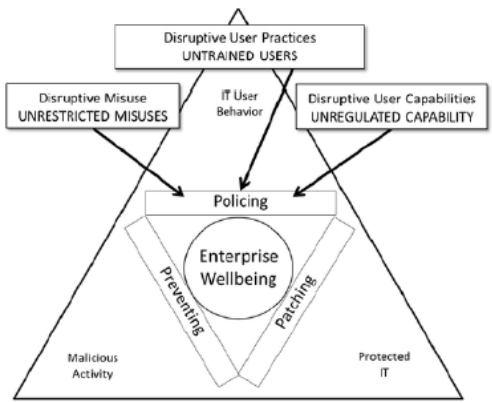
Figure 1. Assessed separately for each threat at each LAN [4]



[4] Hadarics, K.–Gyorffy, K.–Nagy, B.–Bognar, L.–Arrott, A.–Leitold, F. (2017): *Mathematical Model of Distributed Vulnerability Assessement, Security and Protection of Information 2017*. University of Defence, IDET BRNO.

Using these mathematical algorithms, the IT infrastructures, the IT devices, the IT threats can be analysed with relevant parameters. The three, identified factors in the applied model are some factors of the cyber-threats.

Figure 2. Typical sources of IT infrastructure vulnerabilities



There are characteristic and prevalence of the harmful cyber-threats, the vulnerabilities in the IT systems, the user's behaviour risks. [5], [6] The social engineering-based fraud approaches mostly the uninformed person, but without necessary knowledge, the average person or the Youngers can become a victim too.

The weakest link, the human factor and the innocent Youngers in the cybercrime

Nowadays, on the dark side of the Internet, data manipulation, data abuse and other cybercrime are preferred, and the easy-going Youngers promote the spreading of crime. The incorrect user's attitude is a great problem in the protecting IT system. *(Figure 3)*

[[5] Leitold, F.–Arrott, A.–Hadarics, K. (2016): Quantifying cyber-threat vulnerability by combining threats intelligence, IT infrastructure weakness and user susceptibility, 24th Annual EICAR Conference, Nuremberg, Germany, 2016.

[6] Leitold, F.–Arrott, A.–Hadarics, K.: Automating visibility into user behavior vulnerabilities to malware attack, Proceedings of 26th Virus Bulletin International Conference (VB2016), Pp. 16–24, Denver, USA.

[7] 2020 Internet Crime Report, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf, download: January 20, 2021.

[8] Cyber Crime Strategy, Office of Public Sector Information, Information Policy Team, Kew, Richmond, United Kingdom, 2010.

Figure 3. FBI, Internet Crime Report, 2020 [7]

2020 VICTIMS BY AGE GROUP

Victims		
Age Range[7]	Total Count	Total Loss
Under 20	23,186	$70,980,763
20 - 29	70,791	$197,402,240
30 - 39	88,364	$492,176,845
40 - 49	91,568	$717,161,726
50 - 59	85,967	$847,948,101
Over 60	105,301	$966,062,236

The possibilities on the Internet (the openness, the interactive forms, the decentralization and the globalization) contribute to increasing the number of abuses. Analysed items can be defined, such as large-scale infrastructures, such as airport, economic, banking or industrial management system, and a person too. We can analyse states institutions, other organisation, individuals or a child. Therefore, the target point can be anything and anyone, irrespective of institution or person. The cause is wide-ranging, therefore it can be something from a random event or personal motivation to a warning notice or terror plot.

The person who commits some online fault in the IT system can be a hacker, cracker, phreak, cyberpunk, pirate, anarchist or terrorist. Increasingly often that the Youngers commit cybercrime and they don't know it was a crime. Especially a preprogrammed application is activated on their smartphone or computer. This is a shared malicious software which is spreading on the Internet to cause significant damage on other's smart phone or computer. In this case, the young person becomes a victim too who shared the malicious program. The phenomenon is also worrying, because of their age. The young people do not see and do not feel the impact of serious consequences of their actions. The other method is when the target of the malicious person one of the young victim, who feels threatened and unable to escape the bullying. The malicious person is manipulating the victim by the Internet. [8]
There is more and more technical type with which the malicious person cause harm, which is presented in the next figure.

Figure 4. FBI, Internet Crime Report, 2020 [9]

2020 CRIME TYPES

By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	241,342	Other	10,372
Non-Payment/Non-Delivery	108,869	Investment	8,788
Extortion	76,741	Lottery/Sweepstakes/Inheritance	8,501
Personal Data Breach	45,330	IPR/Copyright and Counterfeit	4,213
Identity Theft	43,330	Crimes Against Children	3,202
Spoofing	28,218	Corporate Data Breach	2,794
Misrepresentation	24,276	Ransomware	2,474
Confidence Fraud/Romance	23,751	Denial of Service/TDoS	2,018
Harassment/Threats of Violence	20,604	Malware/Scareware/Virus	1,423
BEC/EAC	19,369	Health Care Related	1,383
Credit Card Fraud	17,614	Civil Matter	968
Employment	16,879	Re-shipping	883
Tech Support	15,421	Charity	659
Real Estate/Rental	13,638	Gambling	391
Advanced Fee	13,020	Terrorism	65
Government Impersonation	12,827	Hacktivist	52
Overpayment	10,988		

Descriptors*		
Social Media	35,439	*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.
Virtual Currency	35,229	

One part of the project has the object to find the correct connection points between the cybercriminals and the human weak points. The perpetrators prefer social engineering solutions because the human factor is the weakest link in information security. In this group of cybercrimes, the leader is a qualified and crafty man. The executors or the perpetrators do not have high-level computer skills, and they often use simple solutions. Cybercriminals are constantly looking for ways to get money, and they cause damage to the weakest links as well. The citizens and the organisations often fall victim to fraud. Nowadays, social engineering fraud-based crime is one of the most profitable underworld businesses. [10] Based on one of the methods the frauds had diddled organisations out of their money. It was claimed that the organizations had an unpaid account and the organizations had to transfer the amount

[9] 2020 Internet Crime Report, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf, download: January 20, 2021.

[10] EUR 8 million, 700 bank accounts and money mules: the little-known tricks of social engineering fraudsters, https://www.europol.europa.eu/newsroom/news/eur-8-million-700-bank-accounts-and-money-mules-little-known-tricks-of-social-engineering-fraudsters, download: January 26, 2019.

to a specified bank account. In this case, they are manipulated by frauds. According to other events, the employers are manipulated to get or to send some of the business secret or personal data to the online fraud.

Of course, it is only could estimate, how much damage it is could cause to the global economy by cybercriminals. Based on the 2016 analysis of Cybersecurity Ventures is estimated at 3 trillion dollars in the 2017 year damages that is could increase at 2021 to 6 billion dollars. The statements it was calculated the direct and indirect damage caused, so the risk or the damage is caused by leak-out of personal data *(Figure 5)*, disclosure of business secrets or critical infrastructure damage. [11]

Figure 5. FBI, Internet Crime Report, 2020 [12]

The management and development of awareness

Unfortunately, we may not be counting on a user's conscious activity. At the end of 2016, 47 percent of the world's population used the Internet (International Telecommunication Union data) (*Figure 6, 7)*. In a larger company with more than a thousand people, they all have access to IT systems. Access and authorization at different levels are very important. It should be taken into account that an ignorant or untrained user is enough and the most important protection is already in danger. A survey of national IT security awareness has found similar results. More than a third part of the workers in the business or the public sector think so that their computers are not potential target of a malicious attack.

[11] Cybersecurity Ventures 2016 Cybercrime Report – Hackerpocalypse: A Cybercrime Revelation, https://www.cyberdefensemagazine.com/cybersecurity-ventures-2016-cybercrime-report-hackerpocalypse-a-cybercrime-revelation/ download: January 26, 2019.

[12] 2020 Internet Crime Report, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf, download: January 20, 2021.

Figure 6. International Telecommunication Union, ICT Facts and Figures 2016 [13]

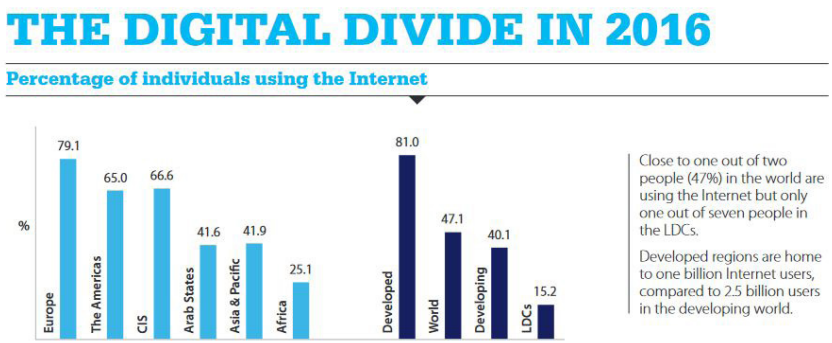
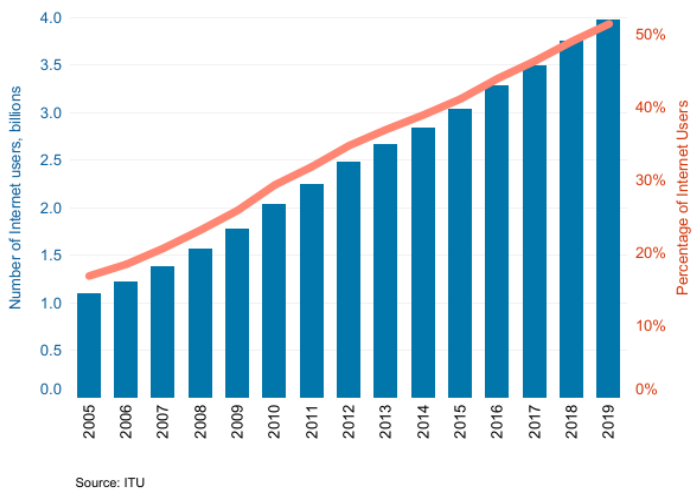


Figure 7. International Telecommunication Union, Statistics, Number of Internet users, 2005–2019 [14]



[13] International Telecommunication Union, ICT Facts and Figures 2016, ITU, Geneva, Switzerland, 2016.

[14] International Telecommunication Union, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, download: January 20, 2021

Regular information security awareness is of great importance in secondary school and at the universities too. The awareness raising and the teaching will strengthen the safe using of applications, applying of the necessary security policy, observing of the essential rules of data protection at the appropriate level which is especially significant in the community of users, system administrators and data controllers. In addition, the objective is the strengthening of the communication and cooperation between different users and operators.

The education sector is becoming an increasing target for cyber-criminals. In 2016, the University of Calgary famously fell victim to a ransomware attack in which it was forced to pay out more than $15,000 to regain access to forcefully encrypted files. It is important to note that cyber-security awareness training must be carried out periodically because a "solve it, do it" approach ineffective, as online criminals are constantly evolving and developing new ways to exploit system vulnerabilities and attack network users. Students are practically born with technology between their hands, but they don't have the information about security. [15] „Schools have a responsibility to prepare kids to be smart, capable and thoughtful digital citizens," said Jacqueline Beauchere, a director in Microsoft's Trustworthy Computing Group. „Not only must students know how to stay safer online at school and at home, but they also must be equipped to deal with the workplace challenges of the digital age. Teachers will need training and support to ensure that they have the skills and confidence to cover these topics in the classroom." There are some opportunities for IT security training for students and employees. For the student, training should be integrated into the school system, while the employee should be provided with further training tailored to his or her abilities.

The European Commission adopted the first Digital Education Action Plan, which focused on formal education, such as primary and secondary schools, and higher education and ENISA covered three priority areas

– making better use of digital technology for teaching and learning,
– developing digital competencies and skills,
– improving education through better data analysis and foresight.

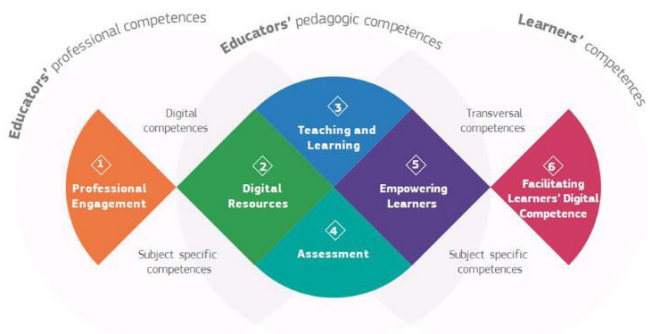
European Union Agency for Network and Information Security (ENISA) has developed the following rules for developing IT security awareness, which are found the next. It is required, that

– basic digital skills and competencies from an early age,
– digital literacy, including tackling disinformation,

[15] 2011 State of Cyberethics, Cybersafety and Cybersecurity Curriculum in the U.S. Survey America's K–12 schools not preparing kids for digital age, study finds, https://www.prnewswire.com/news-releases/2011-state-of-cyberethics-cybersafety-and-cybersecurity-curriculum-in-the-us-survey-121240319.html, download: January 20, 2021.

– computing education,
– good knowledge and understanding of data-intensive technologies, such as artificial intelligence (AI),
– advanced digital skills, which produce more digital specialists,
– ensuring that girls and young women are equally represented in digital studies and careers.

Figure 8. The six competence areas of the DigiCompEdu framework [16]



More than 2700 contributions were received in the open public consultation on the digital education action plan, which took place from 18 June to 4 September 2020. Experiences of learning during the COVID-19 crisis were at the centre of the consultation, which targeted students; parents and carers; the wider public; employers and companies and educators and education and training institution. *(Figure 8, 9, 10)*

[16] Digital Education Action Plan (2021-2027), Resetting education and training for the digital age, https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en, download: May 2, 2021.

[16] Digital Education Action Plan (2021-2027), Resetting education and training for the digital age, https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en, download: May 2, 2021.

Figure 9. Digital Education Action Plan (2021-2027) [16]

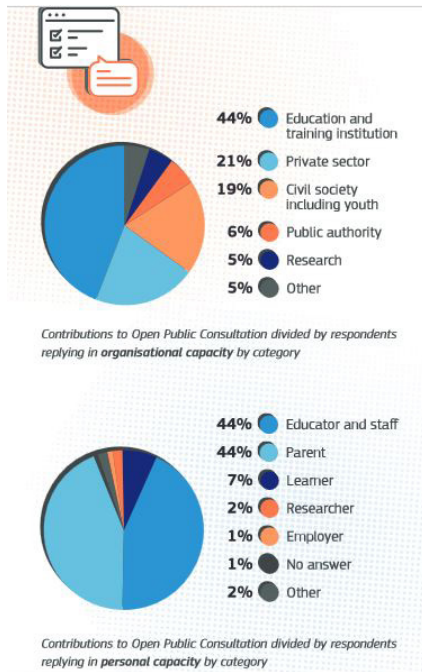


Figure 10. The five competence areas of the DigComp framework [16]

The costs of risk management

Information risk management is more than just a theory because this is a practice. The process of information risk management is used for the project. The most detailed and accurate data is needed to evaluate the risk analysis. The range of data should be complete and the results must be accurate. Thus, it can be assumed that risk management measures and instructions based on analytical results will be appropriate in the IT system. An important part of IT risk management is the periodic survey, the estimation of the position of the IT area. According to reference, it is applied the online survey methods in the topics of Social Engineering, the methods of observation or data mining, the user's activity threats and attack tests for information retrieval methods with monitoring and sampling procedures, the IT risk analysis methods with sampling, qualitative and quantitative ways. Detecting and changing the weak link in the IT system requires increased attention. This is not just a system tool, but also a human aspect. Each risk factor is unique and therefore requires unique solutions.

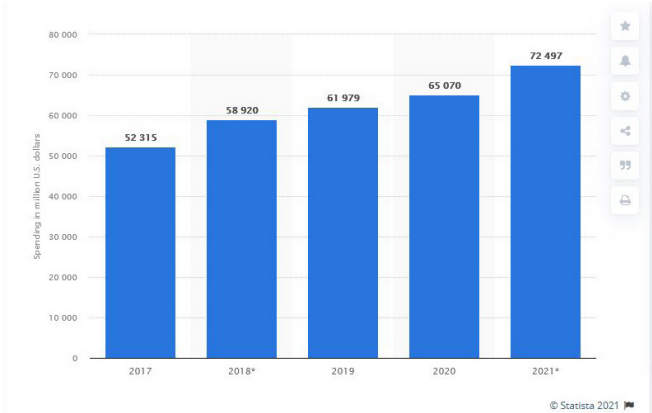
IT risk management is a very important example of the acknowledgement that the possible weaknesses and threats have to treat in the IT world. Today, organizations strive to keep pace with the risk factors of the electronic world (it is presented in the 2014-2015 statistics). [17] In this, there is declared spending more for the project of the information security than in before years. The surveyed companies increased their information security spending by an average of 24 percent in 2015. According to companies the property damage of the informatics incident is reduced between 2014 and 2015 years from 2,7 million dollars to 2,5 million dollars. It had happened of the influence of the information security measures. Based on the statement the 91 percent of companies initiated an information security management system (ISO/IEC 27001 standard based ISMS) with risk analysis and 59 percent of companies purchased cybersecurity services.

[17] Ötvös, G.: *Kiberbiztosítási trendek (Cyber security trends), Biztosítás és Kockázat (Insurance and Risk),* no. 1.,Hungary, 2016.

[18] Worldwide information security services spending from 2017 to 2021, Statista, https://www.statista.com/statistics/217362/worldwide-it-security-spending-since-2010/, download: May 2, 2021.

[19] Gyorffy, K.–Leitold, F.–Arrott, A.: Individual awareness of cyber-security vulnerability – citizen and public servant, Central and Eastern European e|Dem and e|Gov Days, Budapest, Hungary, 2017.

Figure 11. Worldwide information security services spending from 2017 to 2021 [18]



Rising IT security costs *(Figure 10)* also justify the need to develop digital competencies and security awareness behaviours.

Conclusion

Cyberspace and its environment represent a new dimension for our world, where criminal proceedings against cybercrime can be successful. [19] Difficulties in cyberspace are especially the vulnerabilities and the incidents, which exploit them. The negative impact affects not only the life of the employee, public institutions or other organizations but also the lives of households and causes serious economic damage.

It can be only known the potential of cyberspace when it is known the IT vulnerability and the IT threat, and these will be incorporated as a daily activity into our tasks. When the attack options and vulnerability are identified and raised awareness of the attack capabilities and vulnerabilities, and remedial measures are published so the instructions would be a daily routine. The action plan with a simplified version that is easy to learn and series of small steps and the accepting and the applying is facilitated. The secret of the further lies in the online helpdesk and the IT knowledgeable and the security awareness.

The key lesson of the COVID-19 crisis is that digital education should no longer be viewed as an island of its own but considered an integral part of all education and training. The Digital Education Action Plan offers a long-term strategic vision for high-quality, inclusive and accessible European digital education which can be applied both in primary school, in secondary school and the university. By applying the mathematical and digital action map method together, the digital action plan is the Safety competence of DigComp, and the training of the information security awareness can be completed.

Galéria

Németh István fotói (Montenegró)