

37. Országos Tudományos Diákköri Konferencia  
Had- és Rendészettudományi Szekció  
Budapest, 2025. április 22–24.  
Nemzeti Közsolgálati Egyetem  
Hadtudományi és Honvédtisztképző Kar

---

## **NLP ALAPÚ VÉDEKEZÉSI MÓDSZERTAN FEJLESZTÉSE SOCIAL ENGINEERING TÁMADÁSOKKAL SZEMBEN**

Jelige: jelige: NLP

Pályamunka lezárásának időpontja: 2024. 11. 7.

# TARTALOMJEGYZÉK

## Tartalom

|                                                              |              |
|--------------------------------------------------------------|--------------|
| <b>1.ABSZTRAKT.....</b>                                      | <b>4</b>     |
| <b>2.KUTATÁSI JELENTÉS .....</b>                             | <b>5</b>     |
| 2.1. KUTATÁS ELŐZMÉNYEI.....                                 | 5            |
| 2.2. KUTATÁS JELENTÉS .....                                  | 5            |
| 2.3. KUTATÁS JÖVŐKÉPE.....                                   | 5            |
| <b>3.ACM KLASSZIFIKÁCIÓ.....</b>                             | <b>6</b>     |
| <b>4.BEVEZETÉS .....</b>                                     | <b>I</b>     |
| 4.1. BEVEZETŐ GONDOLATOK .....                               | I            |
| 4.2. MOTIVÁCIÓ .....                                         | I            |
| 4.3. EDDIGI KUTATÁSI EREDMÉNYEK ISMERTETÉSE.....             | I            |
| 4.4. SOCIAL ENGINEERING TERMINOLÓGIÁK .....                  | II           |
| 4.5. TECHNOLÓGIAI ALAPOK .....                               | IV           |
| 4.6. GÉPI TANULÓ ALGORITMUSOK RÖVID BEMUTATÁSA .....         | VII          |
| 4.6.1. <i>Klasszifikációs fák</i> .....                      | VII          |
| 4.6.2. <i>Nearest Neighbors</i> .....                        | VIII         |
| 4.6.3. <i>Support Vector Machine Classification</i> .....    | VIII         |
| 4.6.4. <i>Matlab Classification Learner</i> .....            | VIII         |
| <b>5.A TÉMA AKTUALITÁSA .....</b>                            | <b>IX</b>    |
| 5.1. TÉMA AKTUALITÁSA ONLINE FORRÁSOK ALAPJÁN .....          | IX           |
| 5.2. TÉMA AKTUALITÁSA SZAKÉRTŐI MEGKÉRDEZÉS ALAPJÁN .....    | IX           |
| 5.3. TUDOMÁNYREPREZENTÁCIÓ MTMT-BEN 2023 TAVASZ .....        | IX           |
| 5.4. TUDOMÁNYREPREZENTÁCIÓ MTMT-BEN 2023 ŐSZ.....            | X            |
| 5.5. TUDOMÁNYREPREZENTÁCIÓ MTMT-BEN 2024 TAVASZ .....        | XI           |
| 5.6. TUDOMÁNYREPREZENTÁCIÓ MTMT-BEN 2024 ŐSZ.....            | XII          |
| 5.7. TUDOMÁNYREPREZENTÁCIÓ IEEEEXPLORE-BAN 2023 TAVASZ ..... | XIII         |
| 5.8. TUDOMÁNYREPREZENTÁCIÓ IEEEEXPLORE-BAN 2023 ŐSZ.....     | XIV          |
| 5.9. TUDOMÁNYREPREZENTÁCIÓ IEEEEXPLORE-BAN 2024 TAVASZ ..... | XV           |
| 5.10. TUDOMÁNYREPREZENTÁCIÓ IEEEEXPLORE-BAN 2024 ŐSZ .....   | XVI          |
| 5.11. TUDOMÁNYREPREZENTÁCIÓ JSTORE-BAN 2023 ŐSZ .....        | XVI          |
| 5.12. TUDOMÁNYREPREZENTÁCIÓ JSTORE-BAN 2024 TAVASZ.....      | XVII         |
| 5.13. TUDOMÁNYREPREZENTÁCIÓ JSTORE-BAN 2024 ŐSZ .....        | XVIII        |
| 5.14. TUDOMÁNYREPREZENTÁCIÓ SCOPUS-BAN 2023 ŐSZ.....         | XVIII        |
| 5.15. TUDOMÁNYREPREZENTÁCIÓ SCOPUS-BAN 2024 TAVASZ .....     | XIX          |
| 5.16. TUDOMÁNYREPREZENTÁCIÓ SCOPUS-BAN 2024 TAVASZ .....     | XX           |
| 5.17. SCOPUS AI – TÉMA FELDERÍTÉSE .....                     | XX           |
| <b>6.PROBLÉMÁK MEGFOGALMAZÁSA .....</b>                      | <b>XXI</b>   |
| 6.1. PROBLÉMA MEGFOGALMAZÁSA .....                           | XXI          |
| 6.2. HIPOTÉZISEK .....                                       | XXII         |
| <b>7.SZEKUNDER KUTATÁS.....</b>                              | <b>XXIII</b> |
| 7.1. IRODALOMKUTATÁS EREDMÉNYEI.....                         | XXIII        |
| <b>8.PRIMER KUTATÁS.....</b>                                 | <b>XXV</b>   |
| 8.1. SZAKÉRTŐI MEGKÉRDEZÉSEK .....                           | XXV          |
| 8.2. SZAKÉRTŐI INTERJÚK EREDMÉNYEI.....                      | XXVI         |
| 8.3. LAKOSSÁGI MEGKÉRDEZÉS (KÉRDŐÍVVEL).....                 | XXVII        |
| 8.3.1. <i>Módszertan</i> .....                               | XXVII        |
| 8.3.2. <i>Eredmények</i> .....                               | XXVIII       |
| 8.4. KORÁBBI MÉRÉSEK BEMUTATÁSA .....                        | XXXI         |
| 8.4.1. <i>1. Modell</i> .....                                | XXXII        |

|                                    |                                                            |              |
|------------------------------------|------------------------------------------------------------|--------------|
| 8.4.2.                             | 2. Modell .....                                            | XXXIII       |
| 8.4.3.                             | 3. Modell .....                                            | XXXIII       |
| 8.4.4.                             | További modellek sikertelensége.....                       | XXXIII       |
| 8.5.                               | FRISS MÉRÉSI EREDMÉNYEK .....                              | XXXV         |
| 8.5.1.                             | Kártékony Emailek detektálása .....                        | XXXV         |
| 8.5.2.                             | Kártékony SMS-ek detektálása.....                          | XXXVII       |
| 8.6.                               | EMAIL EXPORT-IMPORT ELŐRE PONTOZÁS .....                   | XXXVII       |
| 8.7.                               | ÚJ TÁMADÁSI OSZTÁLYOK LÉTREHOZÁSA .....                    | XXXVIII      |
| 8.8.                               | MÉRÉSEK SZABADON HASZNÁLHATÓ NAGY NYELVI MODELLEKKEL ..... | XXXVIII      |
| 8.8.1.                             | Bard.....                                                  | XXXVIII      |
| 8.8.2.                             | ChatGPT .....                                              | XXXIX        |
| 8.9.                               | SAJÁT MÓDSZER KIDOLGOZÁSA .....                            | XL           |
| <b>9.KONKLÚZIÓ - TÉZISEK .....</b> |                                                            | <b>XLI</b>   |
| <b>10.TÁMOGATÁS .....</b>          |                                                            | <b>XLII</b>  |
| <b>11.IRODALJEGYZÉK.....</b>       |                                                            | <b>XLIII</b> |

## 1. ABSZTRAKT

Ahogy fejlődik az információs technológia, a biztonsági megoldások és a támadások is egyre kifinomultabbá válnak. A technológia megkönnyíti életünket, és a "technológiai bennszülött" kifejezés is kialakult a szingularitás közeledtével. Ezt a fejlődést a támadók is kihasználhatják, mivel az informatikai biztonság előrehaladtával nekik is új módszereket kellett kifejleszteniük. A social engineering, amely pszichológiai vagy pszichológiai és informatikai támadási vektorokat is tartalmazhat, egyre gyakoribb. Ezek a támadások természetüknél fogva nehezen detektálhatók technikai eszközökkel, és megfelelő biztonságtudatosság hiányában közel 100%-os hatékonysággal bírnak célzott támadások esetén. Az egyszerűségük miatt a nem célzott támadásokat könnyebb észlelni, de úgy vélem, hogy ezek száma a jövőben csökkenni fog. Az olyan adatszivárgási botrányok, mint például a Cambridge Analytica esete, nagyszámú felhasználói adatot juttathatnak a dark webre. Ezek az adatok pedig megkönnyítik a célzott támadások automatikus létrehozását.

Célom volt a korábbi alapkutatásom folytatása melynek célja, hogy közvetlenül a támadó emailek és SMS-ek szövegtörzsében található szöveg szerkezetéből, nyelvezetéből, nyelvtani jeleiből és pszichológiai megfogalmazásából képesek legyünk megállapítani, hogy az támadó szándékkal írták-e.

Kutatásomban a természetes nyelvfeldolgozás módszereit hasonlítottam össze, hogy milyen hatékonysággal hasznosíthatóak a kutatás specifikus célok elérésére.

## **2. KUTATÁSI JELENTÉS**

### **2.1. KUTATÁS ELŐZMÉNYEI**

TDK dolgozatomat az Óbudai Egyetem 60. Intézményi Tudományos Diákköri Konferenciája kutatási jelentés formájában készítettem el, mivel ez egy folyamatban lévő kutatás.

A témával három féléve kezdtem el foglalkozni, ahol az Óbudai Egyetem 57. illetve 58. Intézményi Tudományos Diákköri Konferenciáján először bemutattam a témát, illetve feltártam az aggályokat a jelenlegi email biztonsági kihívások kapcsán. Fél év múlva tovább kutatva a témát a problémafelvetésből egyre nagyobb kihívásokat sikerült feltárnom és az elmélet megalkotása után, már elkezdtem méréseket is végezni offenzív szempontból az akkor jó hatékonyságú nyílt forráskódú email biztonsági gépi tanuló modellekkel.

Jelenlegi TDK dolgozatom ezért tartalmaz olyan elemeket (pl.: korábbi mérések és tudomány-reprezentáció) ami jellegéből fakadóan egy az egyben át lettek emelve korábbi TDK dolgozataimból. Ezek esetében, hogy a források ne vesszenek kétszer fogom hivatkozni azokat a részeket. Egyszer a saját TDK dolgozatom hivatkozása, hogy elkerüljem az önplágiumot, egyszer pedig a tényleges forrást. [23]

### **2.2. KUTATÁS JELENTÉS**

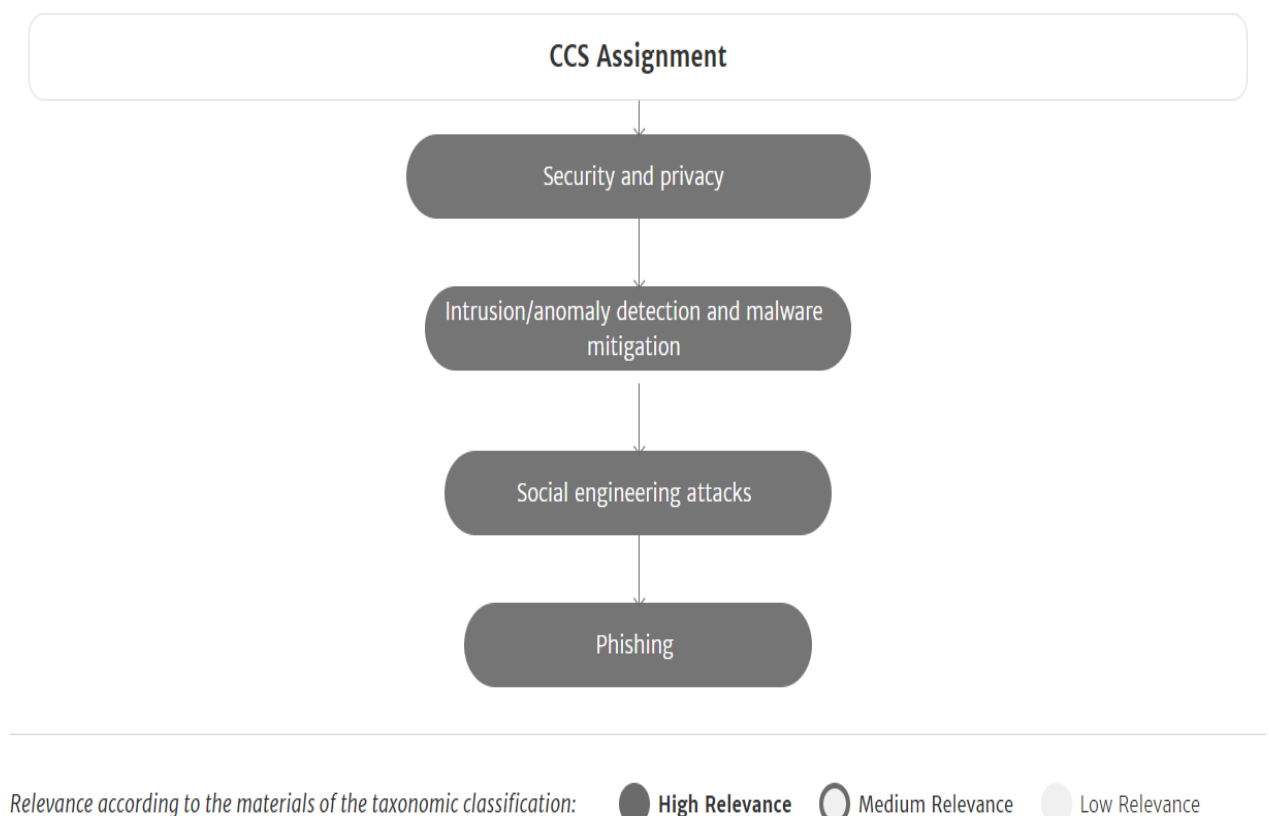
Jelenlegi kutatásomban saját mérései eredményeimet értékelve elkezdtem gyakorlati konklúziókat levonni és további irányokat kijelölni. [23]

### **2.3. KUTATÁS JÖVŐKÉPE**

Kutatásom eddig korlátja legfőképpen a rossz minőségű és kevés adatot tartalmazó adatkészlet volt, ami nyílt forrásból gyakran nem is volt elérhető. A 2024-es ITBN konferencián [24] az Europol kiberbűnözéssel foglalkozó szakértője nyilatkozott arról, hogy a kiberbűnözők nagy része a nagy nyelvi modellek fejlődésének köszönhetően már nem affiliációs csoportokban dolgozik, hanem Ők is nagy nyelvi modelleket használnak arra, hogy támadó emaileket generáljanak. Eddig elvetettem azt a lehetőséget, hogy szintetikus adatokat használjak kutatásomhoz, viszont ezen a ponton az Europol szakértőjének nyilatkozata alapján a generált adatok már nem tekinthetők szintetikusnak, mivel ezt használják a kiberbűnözők is. A következő féléves kutatásomban ezért én is nagy nyelvi modellekkel fogok adatkészletet generálni.

### 3. ACM KLASSZIFIKÁCIÓ

„Az Országos Tudományos Diákköri (OTDT) Tanács javaslata alapján elkészítettem az ACM (Association for Computing Machinery) a számítási klasszifikációs rendszerben (CCS - Computing Classification System) a kutatásom polihierarchikus ontológiáját.” [1] [23]



1. ábra ACM klasszifikáció

## **4. BEVEZETÉS**

### **4.1. BEVEZETŐ GONDOLATOK**

„Az IPAR 4.0 közepén és az IPAR 5.0 közeledtével egyre rohamosabban fejlődik az információ technológia, de vajon az általános biztonságunk is olyan exponenciális mértékben fejlődött mint, ahogy a technológiák egy új ipari forradalom kezdetén?

Sajnos erre az esetek nagy részében nem tud válaszolni a tudomány. Rengeteg szakirodalom, valamint saját kutatásaim és tapasztalataim is bizonyítják azt, hogy nem vagyunk képesek a biztonság macska egér játékában az egér sebességét megközelíteni. Különösen olyan esetekben, amikor a támadók már nem csak informatikai támadási vektorokat alkalmaznak, hanem pszichológiával ötvözik támadásaikat, akkor az eddig csak informatikai biztonságra fókuszáló védekező kollégáknak esélyük sem lesz arra, hogy felvegyék a harcot a modern szemléletmódú támadásokkal.

A gépi tanulási technológiák rohamos fejlődése, különösen a nagy nyelvi modellek (pl.: OpenAI ChatGPT, Google Gemini) áttörést jelentettek a természetes nyelvfeldolgozás (NLP) tudományterületen, ami most a biztonság, Blue Team oldalán számunkra is hasznos lehet, hogy megpróbáljuk felvenni a harcot az új képességekkel felvértezett kibertámadókkal szemben. „[23]

### **4.2. MOTIVÁCIÓ**

„Mindenkinek van olyan, ami nem hagyja aludni esténként.

Engem az zavart, hogy nem tudjuk műszakilag magas hatékonysággal kivédeni a Social Engineering támadásokat és csakis kizárólag a humán alapú biztonságtudatossági képzéseket tudjuk erre a célra használni. Úgy gondoltam, hogy mérnök hallgatóként elkezdek megoldást találni erre a kihívásra! „[23]

### **4.3. EDDIGI KUTATÁSI EREDMÉNYEK ISMERTETÉSE**

„Gimnazista koromban a Kutató Diákok Országos Szövetségénél végeztem kutatást Social Engineering témában, ahol azt vizsgáltam milyen típusú támadások hogyan érintik a KKV-kat és az állami szereplőket. Valamint, hogyan lehet az ilyen támadások ellen védekezni. A fő konklúziója ennek a majdnem egy éves kutatásnak az lett, hogy jelenleg biztonságtudatossági oktatásokkal és ezen oktatások hatékonyságának visszamérésével lehet egyedül megküzdenni a

Social Engineering támadásokkal szemben. A Kutató Diákok Országos Szövetsége által szervezett 'TUDOMÁNYOS DIÁKKÖRÖK XXII. KÁRPÁT-MEDENCEI KONFERENCIÁJA TUDOK 2022 Műszaki- és reáltudományi Tematikus Konferencia'-án, a 'TUDOMÁNYOS DIÁKKÖRÖK XXII. KÁRPÁT-MEDENCEI KONFERENCIÁJA (TUDOK)' c. konferencián, valamint a 'X. KUTDIÁK TUDOMÁNYOS HÉTVÉGE - XX. KutDiák Tudományos Esszépályázat'-on volt alkalmam bemutatni eredményeimet 2022 tavaszán. Ebből a kutatásból témavezetőm felkérésére cikket írtam a Biztonságtudományi Szemlében 'Hogyan változtatta meg a XXI-ik századi kibervédelmet a Social Engineering?' címmel, ahol összefoglaltam eddigi kutatási eredményeimet a nyilvánosság számára is. 2022-ban mikor egyetemista lettem tovább folytattam kutatásomat, immár olyan műszaki megoldás kutatását tűztem ki célként amit az eddigi kutatásom szerint még nem létezett vagy legalábbis nem terjedt el. Az Óbudai Egyetem 57. Tudományos Diákköri Konferenciáján prezentáltam továbbá 'Mesterséges intelligencia alapú email biztonsági megoldások alacsony hatékonyságának gyökér okainak vizsgálata Social Engineering támadások során' címmel. Majd az 58 és 59.-ik ITDK-ra is tovább kutattam az eredményeimet. Ezek a TDK dolgozatok alapozták meg a mostani kutatásomat, így a továbbiakban részben vagy egészben azon részeket, amik még most is relevánsak idézni fogok belőle. [23]

#### **4.4. SOCIAL ENGINEERING TERMINOLÓGIÁK**

„A Social Engineering kifejezés definíciója kapcsán egy jól ismert szakértő Christopher Hadnagy „The Art of Human Hacking” című könyvében leírt definícióját fogadom el dolgozatomban, amely a következő: „A Social Engineering a befolyásolás és rábeszélés eszközével megteszti az embereket, manipulálja vagy meggyőzi őket, hogy a Social Engineer tényleg az, akinek mondja magát. Ennek eredményeként a Social Engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.” [3] Mivel jelenlegi ismereteim szerint nincs általánosan elfogadott fordítása a magyar szaknyelvben (legtöbbször pszichológiai manipulációt tartalmazó támadásként szokták használni), ezért az angol Social Engineering (röviden SE) kifejezést fogom a továbbiakban használni. A Social Engineering támadások tárháza nagyon széles, emiatt ebbe a TDK dolgozatomba nem kívánok belemenni az összes támadási típus ismertetésébe. A támadásokat a hazai és nemzetközi szakirodalom széles körben részletezi. Nemzetközi szakirodalom kapcsán Christopher Hadnagy fent említett könyve g című könyve, hazai szakirodalom kapcsán pedig Tóth Tamás folyóirat cikke [5] dolgozza fel a Social Engineering támadásokat, valamint én is foglalkoztam

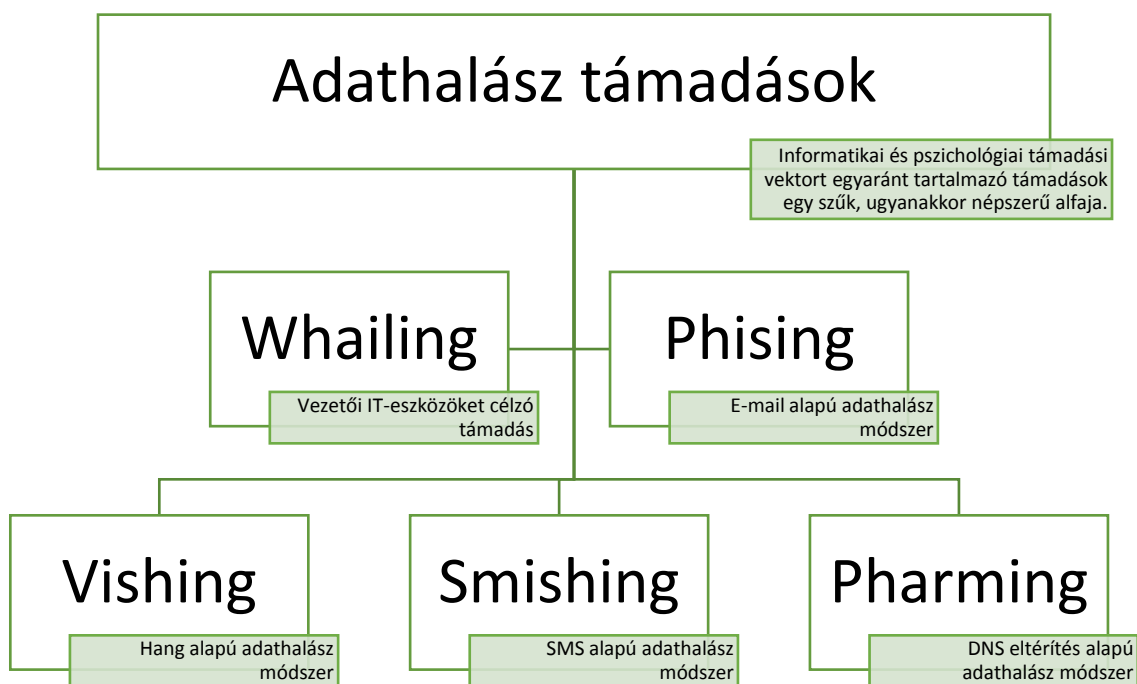
vele korábbi kutatásom során „[6][23]. Amivel első körben foglalkozni szeretnék TDK dolgozatomban azok az adathalász támadások. Az adathalász támadások során a támadó valamilyen



2. ábra, szerző által készített, példa a Netflixes Smishingre

(jellemzően infokommunikációs csatornákon, de volt példa papír alapú adathalásztatra is [7]) módon meggyőzi az áldozatot, hogy adja meg az adatait valamilyen célból olyan legendával, mely nem kelt gyanút az áldozatban. Példa lehet erre a manapság népszerű Netflix-es vagy GLS-es csalások emailben és SMS-ben egyaránt. [23]

Az adathalász támadásokat Tóth Tamás módszere alapján klasszifikáltam [5, pp 95-96] a következő csoportokra:



3. ábra szerző által készített [23]

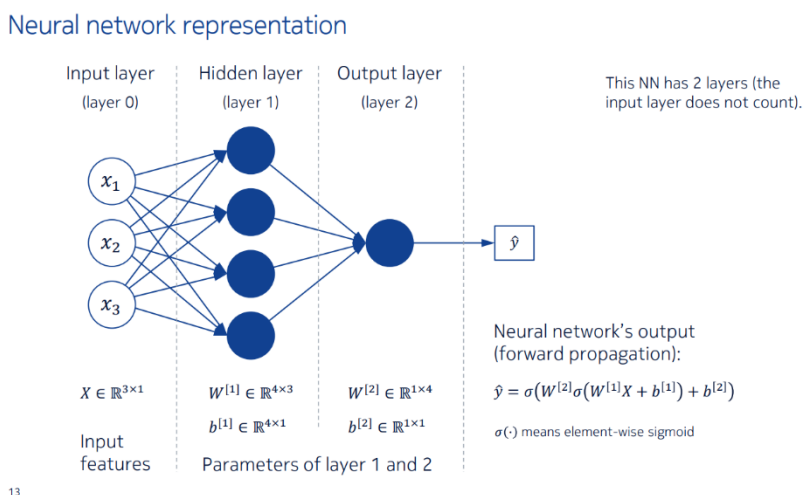
Ezen belül is első sorban a Phishing-el, másodsorban pedig a Smishing-el a későbbiekben. Ezeket hasonlóan a Social Engineering-hez angolul fogom használni, mivel jelenleg nincs elterjedt és egységes magyar nyelvű kifejezés, ami egy szóban lefedné. [23]

#### 4.5. TECHNOLÓGIAI ALAPOK

A mély tanulás története az 1940-es évekig nyúlik vissza, amikor Warren McCulloch és Walter Pitts alkották meg az első mesterséges neuronhálózat elméletét. Azonban a módszer korai éveiben a számítási kapacitás korlátozott volt, és a kutatások lassan haladtak. Az igazi ugrást az 1980-as években tapasztaltuk, amikor a visszaterjesztéses neurális hálózatok (RNN) és a konvolúciós neurális hálózatok (CNN) megjelentek. [21] [23]

Az igazi forradalmat azonban a 21. század elején hozta el a mély tanuláshoz nevezett terület, különösen a mély neurális hálózatok terjedésével. A GPU-k és nagyobb adathalmazok elérhetősége lehetővé tette a mély neurális hálózatok hatékonyabb tanítását. 2012-ben például a ImageNet versenyen AlexNet nevű mély neurális hálózat nyert, jelentős teljesítményjavulást mutatva a klasszikus gépi tanulási módszerekhez képest [22] [23]

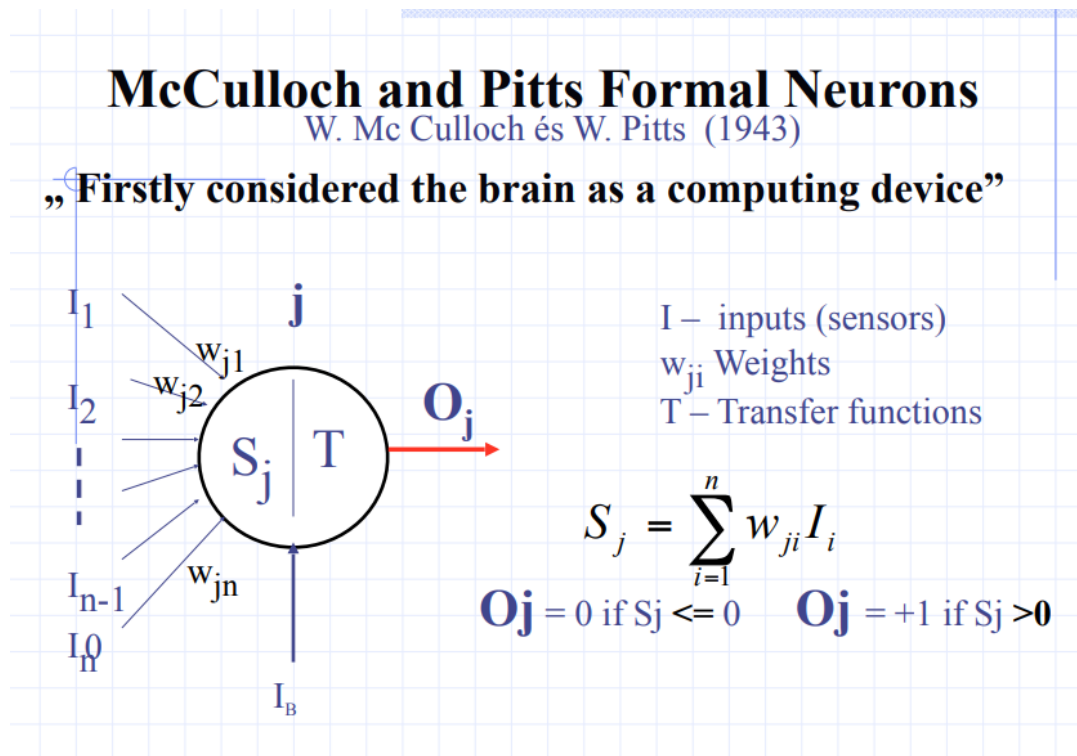
A mai gépi tanulás alapját a neurális hálók adják. Ezek a hálók neuronokból állnak. Rendelkeznek bemeneti, kimeneti és úgynevezett rejtett rétegekkel (ez az összes réteg ami a bemeneti és a kimeneti között van).[23][26]



4. ábra Neurális háló reprezentációja [26]

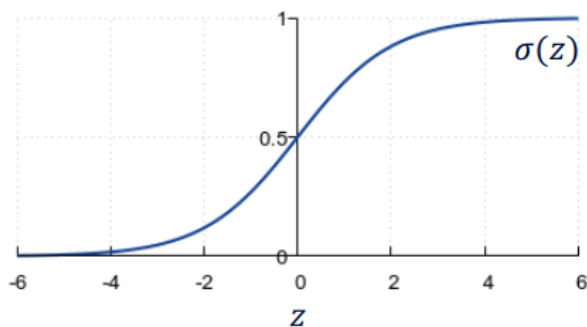
A neuronok általános felépítése az lenti képen látható. Egy neuronnak általánosan vannak bemenetei, amihez súly érték van párosítva. Azért van erre szükség, hogy különböző súllyal

lehesen figyelembe venni a különböző bemeneti értékeket. Ezáltal könnyen módosíthatóvá válnak a bemeneti értékek.



5. ábra McCulloch and Pitts Formal Neurons [27]

Az átviteli vagy aktivációs függvények azok, amik a végső műveleteket elvégzik a neuronokban. Ezek közül a 3 legnépszerűbb a Sigmoid átviteli függvény [23][26]:

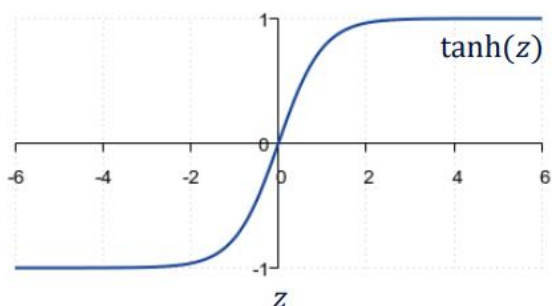


$$\sigma(x) = \frac{1}{1 + e^{-x}}$$

6. ábra Sigmoid átviteli függvény ábrája [26]

A sigmoidot leginkább a kimeneti rétegben alkalmazzák bináris klasszifikáció esetén. [23][26]

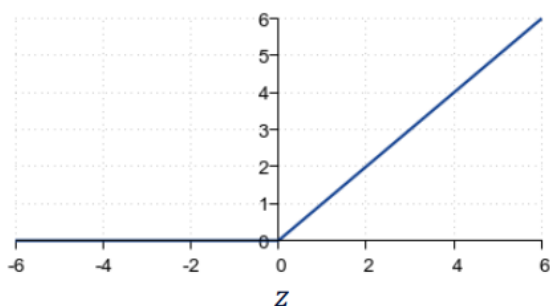
A Tahn függvény szinte mindig jobb eredményt hoz a sigmoidnál és gyakran a rejtett rétegben használják [23][26]:



$$\sigma(z) = \frac{e^z - e^{-z}}{e^z + e^{-z}}$$

7. ábra Tahn függvény ábrázolása [26]

Gyakori választás, főleg hatékonysági okokból kifolyólag a ReLU (rectified linear unit) átviteli függvény. Ez felgyorsítja a neurális hálót, mivel kevésbé számítás igényes, mint a korábbi kettő. [23][26]



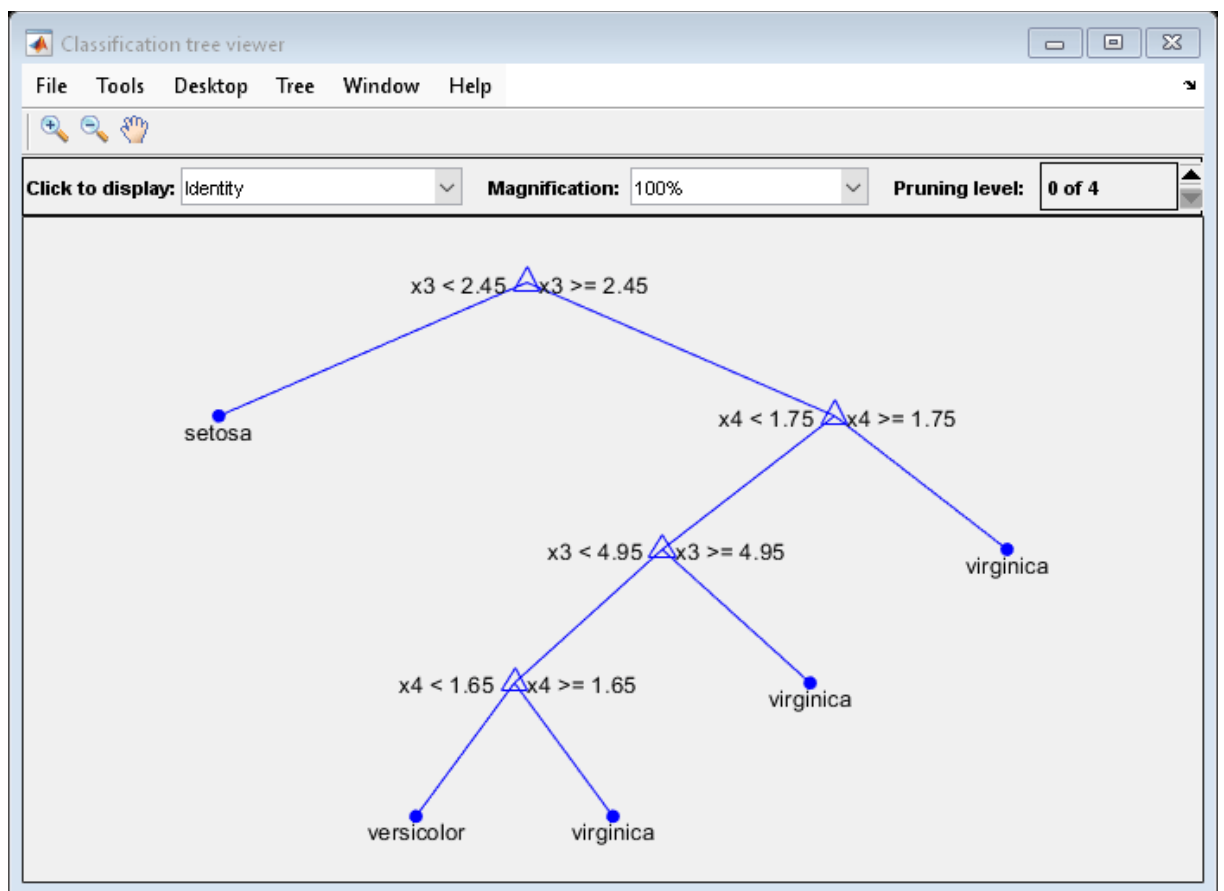
$$\sigma(z) = \max(0, x)$$

8. ábra ReLU függvény ábrázolása [26]

## 4.6. GÉPI TANULÓ ALGORITMUSOK RÖVID BEMUTATÁSA

### 4.6.1. Klasszifikációs fák

A klasszifikációs fák (vagy döntési fák) egy hierarchikus szerkezetű osztályozási módszert képviselnek, amely az adatokat egymást követő, bináris döntésekkel bontja fel. A fa csomópontjai egy-egy kérdést vagy szabályt tartalmaznak, amelyek alapján elágazások keletkeznek, míg a levelekben található az osztályokhoz tartozó előrejelzések. Multiosztályos tanulási feladatoknál a fa minden ága egy adott osztályhoz vezethet, vagy egy bináris fa esetén különféle osztályokhoz rendeljük hozzá a leveleket. [32]



9. ábra Klasszifikációs fák grafikus ábrázolása általános példával. Szerző Matlab: [31]

#### 4.6.2. Nearest Neighbors

A k-legközelebbi szomszéd (k-Nearest Neighbors, k-NN) algoritmus egy egyszerű, ám hatékony gépi tanulási módszer, amely az új adatpont osztályát a tanulóhalmazban található legközelebbi

k pont osztályai alapján határozza meg. Az algoritmus az adatok közötti távolságot (gyakran az euklideszi távolságot) használja, és az új pont osztályát a k legközelebbi szomszéd szavazatai alapján határozza meg.

Az euklideszi távolság képlete két x és y pont között:

$$d(x, y) = \sqrt{\sum_{i=1}^n (x_i - y_i)^2}$$

Az előrejelzés az adott x pontra a legtöbb szavazatot kapott osztály szerint történik.

[32]

#### 4.6.3. Support Vector Machine Classification

Support Vector Machine (SVM) egy felügyelt tanulási algoritmus, amely két vagy több osztály közötti elválasztó határvonal (hipersík) megtalálására szolgál. Az SVM célja az osztályok közötti margin maximalizálása, azaz a legközelebbi adatpontok és az elválasztó sík közötti távolság növelése. Az optimalizálás a következőképpen történik: ha adottak az  $x_i$  adatpontok és  $y_i \in \{-1, +1\}$  osztályok, akkor az SVM megoldja a következő optimalizálási feladatot:

$$\min_{\mathbf{w}, b} \frac{1}{2} \|\mathbf{w}\|^2$$

$$\text{a } y_i(w * x_i + b) \geq 1$$

feltétel mellett.

#### 4.6.4. Matlab Classification Learner

A saját készítésű mérések nagy részét a Matlab keretrendszer Classification Framework szoftvercsomaggal készítettem, ami a fent bemutatott algoritmusokon kívül sok mást is tartalmaz. Azért esett erre a választásom, mivel gyors prototipizálást tesz lehetővé és a mérések sokkal pontosabban tesztelhetőek és értékelhetőek mint más megoldások esetében. Valamint szintén gyorsítja a K+F+I folyamatot, hogy GUI-val rendelkezik és nem kell mindent kézzel megírni, ami miatt koncentrálnunk a valódi problémák megoldására.

## **5. A TÉMA AKTUALITÁSA**

### **5.1. TÉMA AKTUALITÁSA ONLINE FORRÁSOK ALAPJÁN**

„A Social Engineering alapú támadások évről évre nagyobb számban jelennek meg és a TerraNova Security szerint a 2022-es évben az azonosított phishing támadások 96%-a [2] emailen keresztül érte a szervezeteket, ezért különösen időszerűnek tartottam ezen témával való foglalkozást.” [27]

Továbbá megvizsgáltam az egyik legnépszerűbb megoldást, amit phishing támadások ellen tudunk alkalmazni, ez a Cisco Talos Intelligence Group által működtetett PhishTank [23] ami korábban már ismert, többnyire nagy tömeg számára kiküldött adathalász oldalakat tud azonosítani, amely tovább igazolja azon hipotézisemet, hogy jelenleg a technológia nem képes kiszűrni a célzott támadásokat, pusztán a nagy tömegeket elérő támadás hullámokat. [23]

### **5.2. TÉMA AKTUALITÁSA SZAKÉRTŐI MEGKÉRDEZÉS ALAPJÁN**

„Továbbá személyesen is volt alkalmam rövid interjú erejéig megkérdezni egy ISO 27001-es<sup>1</sup> auditort, egy információbiztonsági vezetőt, egy információbiztonsági tanácsadót, egy információbiztonsági szakértőt, egy telekommunikációs cég üzletágvezetőjét és egy szintén telekommunikációs cég vezető kutató mérnökét a témáról és mind a hat interjú alatt azt a visszajelzést kaptam, hogy az általuk működtetett email biztonsági megoldások meglehetősen primitív elven működnek és nem képesek feltétlen az ígért számokat hozni. Megerősítettek benne, hogy érdemes foglalkoznom a témával. Interjúim során kiemelném, hogy a megkérdezettek között vegyesen voltak a versenyszférában és a közigazgatásban egyaránt dolgozók, ezzel növelve a kis mintám reprezentációját.” [23]

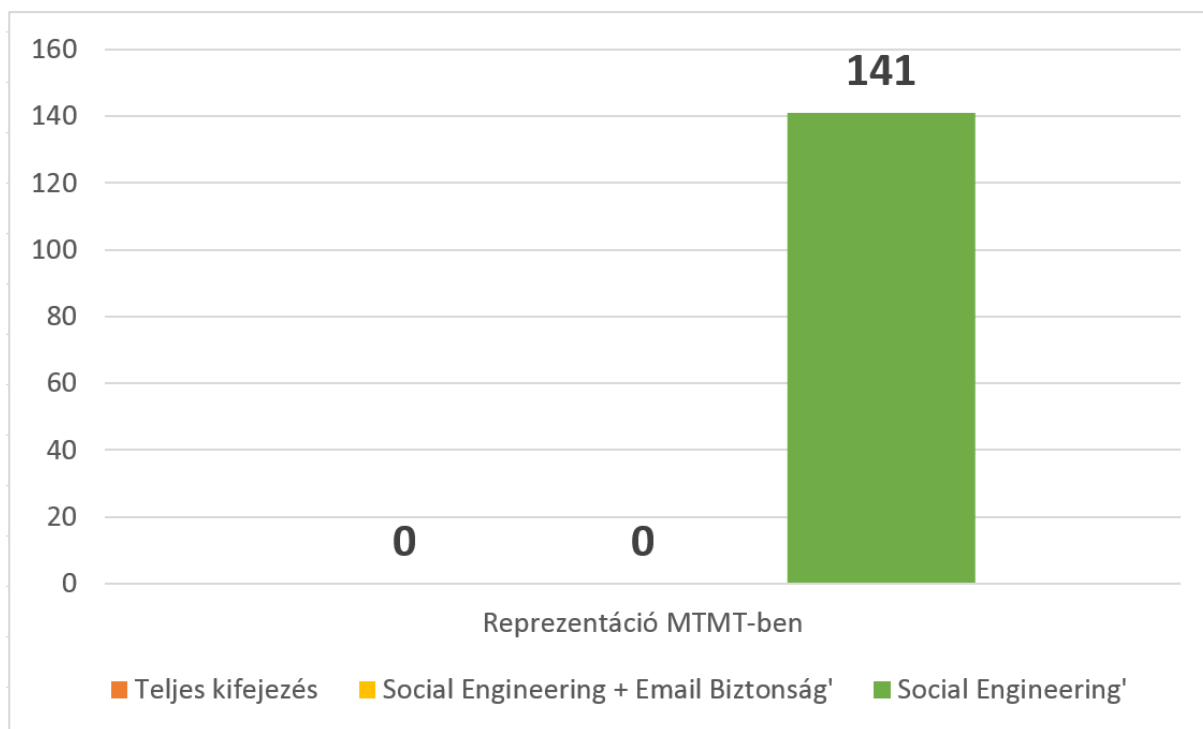
### **5.3. TUDOMÁNYREPREZENTÁCIÓ MTMT-BEN 2023 TAVASZ**

A Magyar Tudományos Művek Tárának adatbázisában 2023 májusában a kulcsszavakra való keresést végeztem. Az alábbi kulcsszavakra kerestem együttesen: "Social Engineering", "Email biztonság" és "mély tanulás". Sajnálatos módon nem sikerült találatokat találnom. Az "Social Engineering" és "email" kulcsszavakra is eredménytelen volt a keresés. Azonban a "Social Engineering" kulcsszóra már jelentős mennyiségű találat érkezett, összesen 141 darab. Ezek között tudományos publikációk és konferencia előadások is szerepeltek szép számban. A "Email biztonság" és "mély tanulás" kulcsszavak keresése is nullás eredményt hozott az MTMT

---

<sup>1</sup> A Nemzetközi Szabványügyi Szervezet információ biztonsági menedzsment szabványa

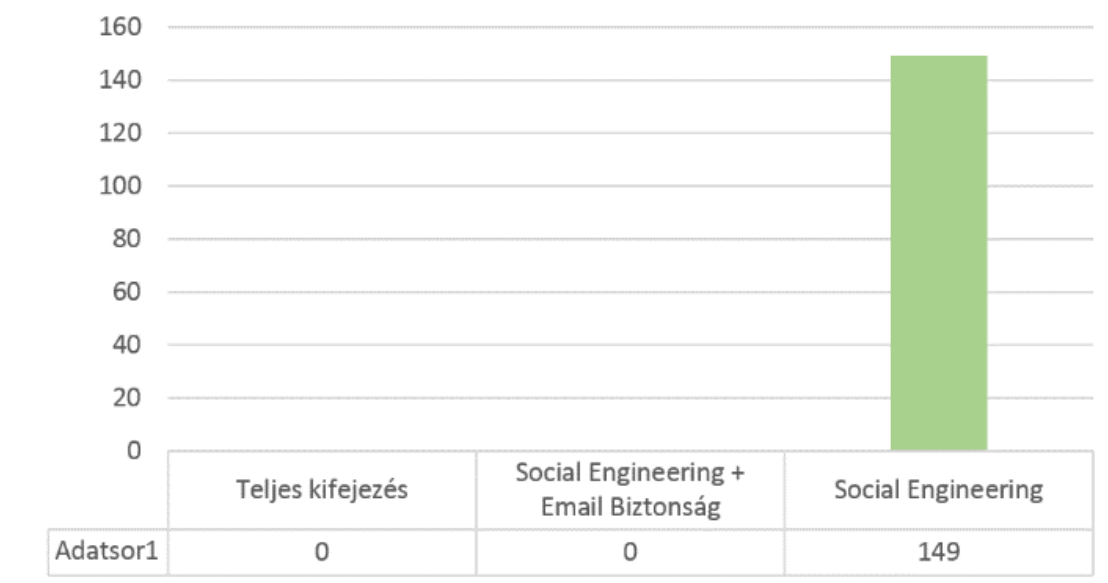
rendszerében. Ezek alapján megállapítottam, hogy Magyarországon ezek a témák 2023 elején kevésbé kutatott területek. [23]



#### 5.4. TUDOMÁNYREPREZENTÁCIÓ MTMT-BEN 2023 ŐSZ

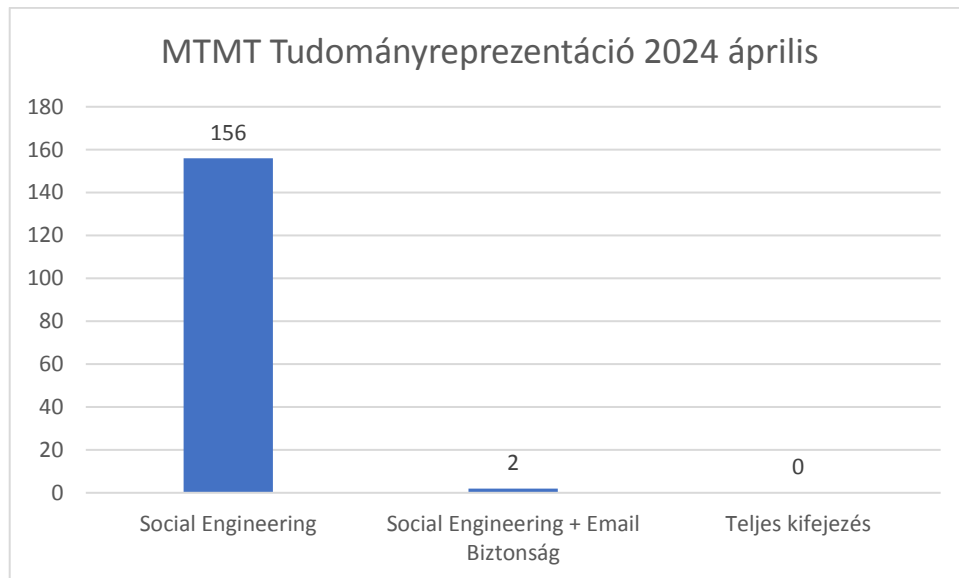
2023 novemberében újra elvégeztem a kulcsszavakra való keresést. Itt is ugyanúgy végeztem el a kulcsszavas keresést. Az alábbi kulcsszavakra kerestem együttesen: "Social Engineering", "Email biztonság" és "mély tanulás". Sajnálatos módon nem sikerült találatokat találnom. Az "Social Engineering" és "email" kulcsszavakra is eredménytelen volt a keresés. Azonban a "Social Engineering" kulcsszóra már jelentős mennyiségű találat érkezett, 149 darab. Ezek között tudományos publikációk és konferencia előadások is szerepeltek szép számban. A "Email biztonság" és "mély tanulás" kulcsszavak keresése is nullás eredményt hozott az MTMT rendszerében. Ez alapján levontam azt a konklúziót, hogy Magyarországon kis mértékben kutatták ezt a témát a korábbi trendekkel szemben. [23]

### MTMT tudományreprezentáció 2023 november



#### 5.5. TUDOMÁNYREPREZENTÁCIÓ MTMT-BEN 2024 TAVASZ

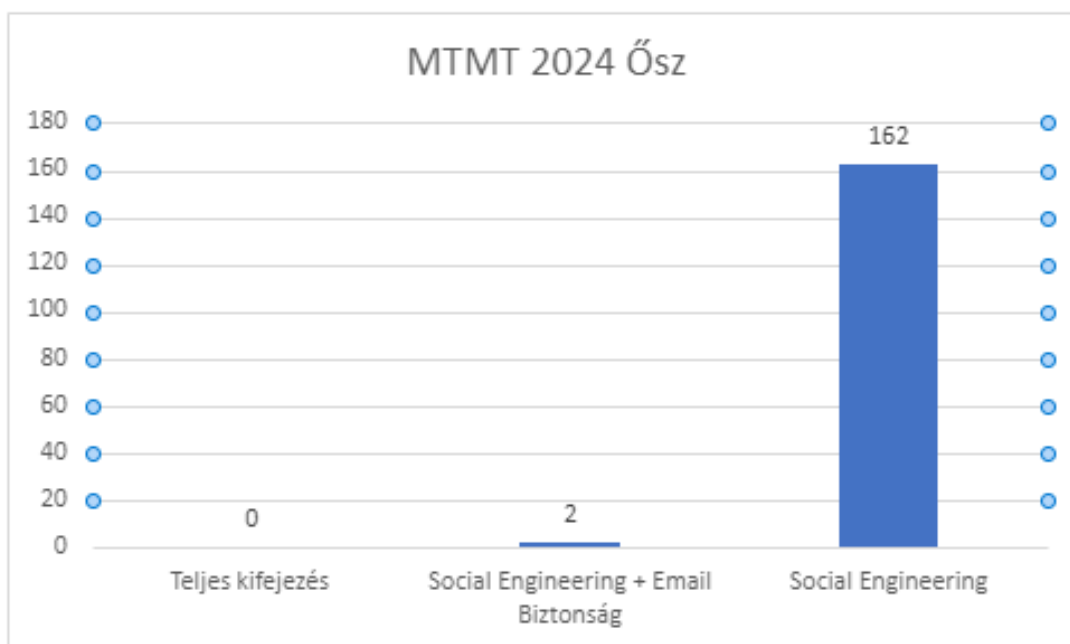
2024 áprilisában újra elvégeztem a kulcsszavakra való keresést. Itt is ugyanúgy végeztem el a kulcsszavas keresést. Az alábbi kulcsszavakra kerestem együttesen: "Social Engineering", "Email biztonság" és "mély tanulás". Sajnálatos módon nem sikerült találatokat találnom. Az "Social Engineering" és "email" kulcsszavakra ugyan kaptam 2 találatot, de mindkettő konferencia előadás hozzám köthető, ezért ezt nem tekintem számomra releváns találatnak. Azonban a "Social Engineering" kulcsszóra már jelentős mennyiségű találat érkezett, 149 darab. Ezek között tudományos publikációk és konferencia előadások is szerepeltek szép számban. A "Email biztonság" és "mély tanulás" kulcsszavak keresése is egy eredményt kaptam, viszont ez is hozzám köthető konferencia előadás, ezért ezt sem tekintem releváns adatnak. Ez alapján levontam azt a konklúziót, hogy Magyarországon kis mértékben kutatták ezt a témát és jelenleg érdemes vele foglalkozni. [23]



## 5.6. TUDOMÁNYREPREZENTÁCIÓ MTMT-BEN 2024 ŐSZ

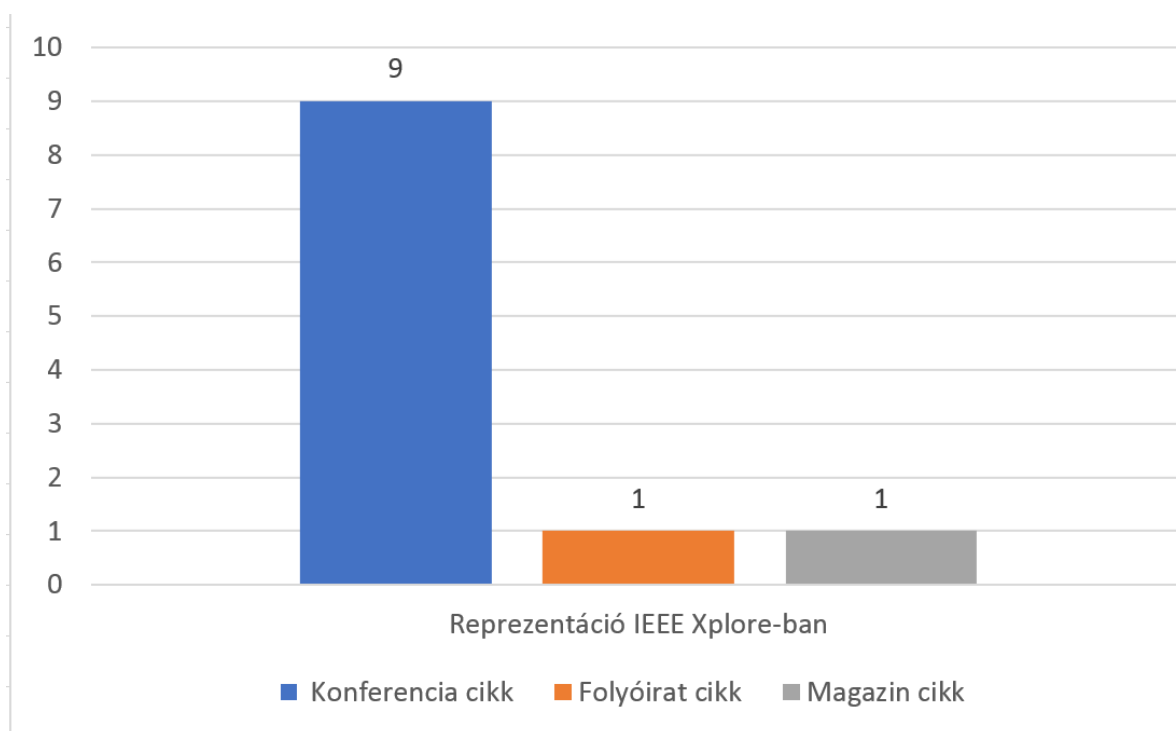
2024 novemberében újra elvégeztem a kulcsszavakra való keresést. Itt is ugyanúgy végeztem el a kulcsszavas keresést. Az alábbi kulcsszavakra kerestem együttesen: "Social Engineering", "Email biztonság" és "mély tanulás". Sajnálatos módon nem sikerült találatokat találnom. Az "Social Engineering" és "email" kulcsszavakra ugyan kaptam 2 találatot, de mindkettő konferencia előadás hozzám köthető, ezért ezt nem tekintem számomra releváns találatnak. Azonban a "Social Engineering" kulcsszóra már jelentős mennyiségű találat érkezett, 156 darab. Ezek között tudományos publikációk és konferencia előadások is szerepeltek szép számban. A "Email biztonság" és "mély tanulás" kulcsszavak keresése is egy eredményt kaptam, viszont ez is hozzám köthető konferencia előadás, ezért ezt sem tekintem releváns adatnak.

Ez alapján levontam azt a konklúziót, hogy Magyarországon kis mértékben kutatták ezt a témát és jelenleg érdemes vele foglalkozni. Valamint a Social Engineeringgel kapcsolatos kutatások lassan, de növekednek.



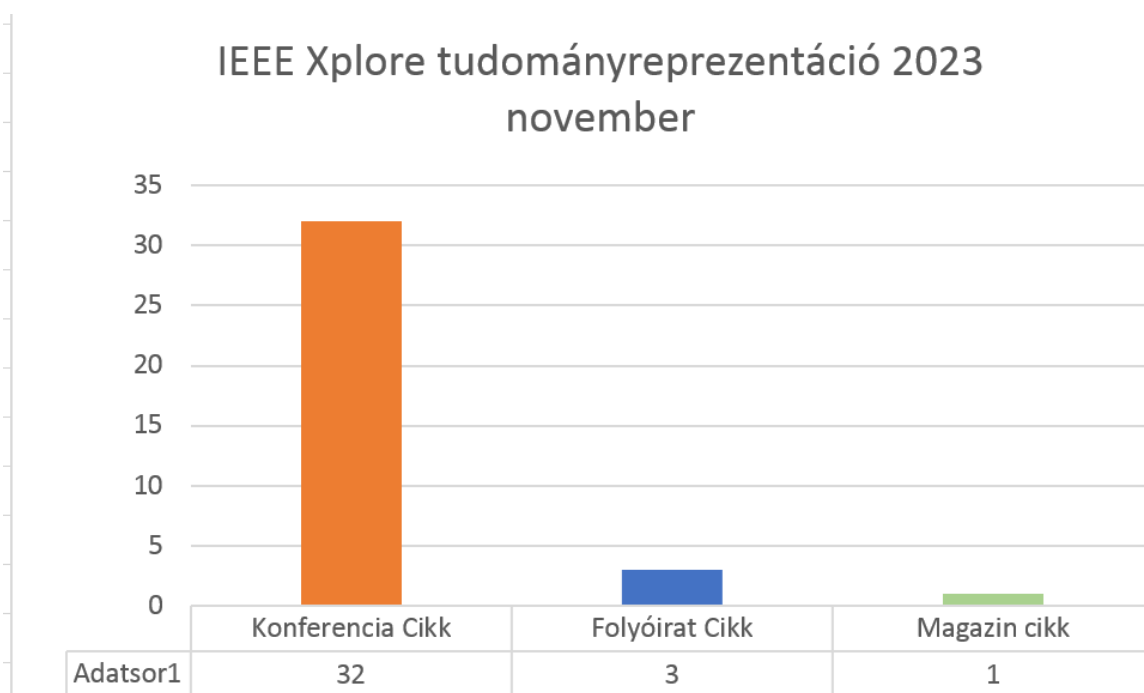
### 5.7. TUDOMÁNYREPREZENTÁCIÓ IEEEEXPLORE-BAN 2023 TAVASZ

Az IEEE Xplore adatbázisban is megvizsgáltam a téma reprezentációját. Mind három kifejezést tartalmazó keresést indítottam a fejlett keresési módban (advanced search: ("All Metadata":Social Engineering) AND ("All Metadata":Email security) AND ("All Metadata":Deep Learning)) melynek során 11 találatot kaptam vissza az IEEE Xplore kereséséből, ebből 9 konferencia cikk, 1 folyóirat cikk és egy magazin cikk eloszlásban voltak. A fent említett találatok közül egy 2019-es, egy-egy 2020 és 2021-es, a többi pedig 2022-ben készült. Ezáltal arra a megállapításra jutottam, hogy a tématerület nemzetközi kutatása sem jelentős és csak az elmúlt években kezdtek el vele foglalkozni. [23]



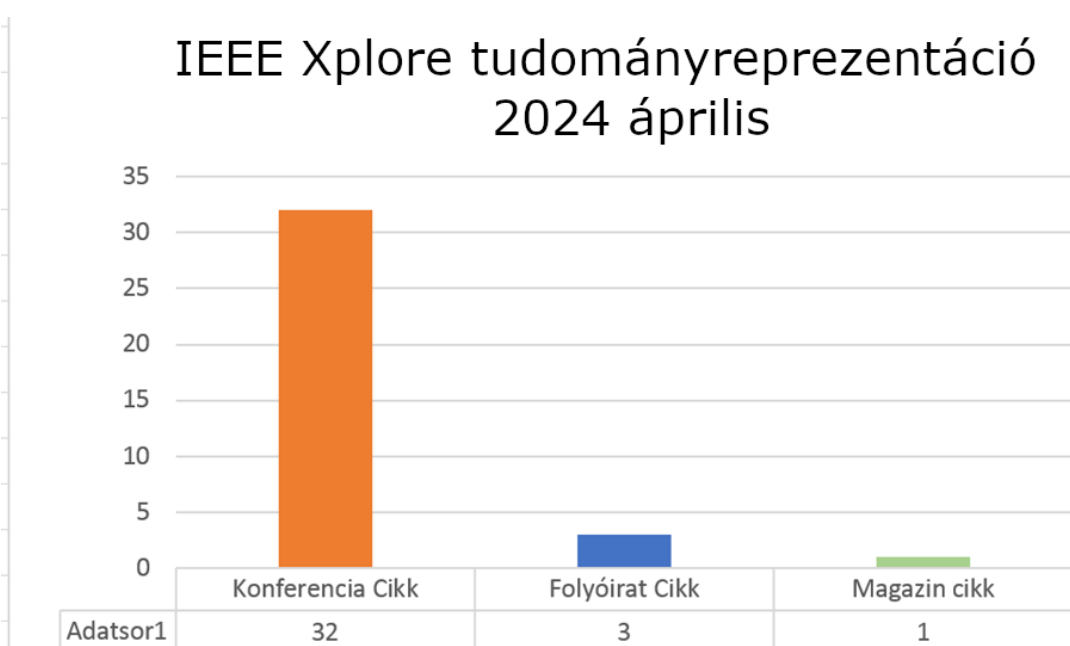
#### 5.8. TUDOMÁNYREPREZENTÁCIÓ IEEEEXPLORE-BAN 2023 ŐSZ

2023 novemberében szintén megvizsgáltam a téma reprezentációját az IEEE Xplore adatbázisban. Az előző kereséssel equivalensen mind a három kifejezést tartalmazó keresést indítottam a fejlett keresési módban (advanced search: ("All Metadata":Social Engineering) AND ("All Metadata":Email security) AND ("All Metadata":Deep Learning)) melynek sorn 36 találatot kaptam. Ez a tavaszi 11-nél 25-el több. Ebből arra a következtetésre jutottam, hogy a téma elkezdett a nemzetközi mérnöki adatbázisban felkapott lenni. Releváns vele most foglalkozni és jelenleg aktívan kutatott terület. [23]



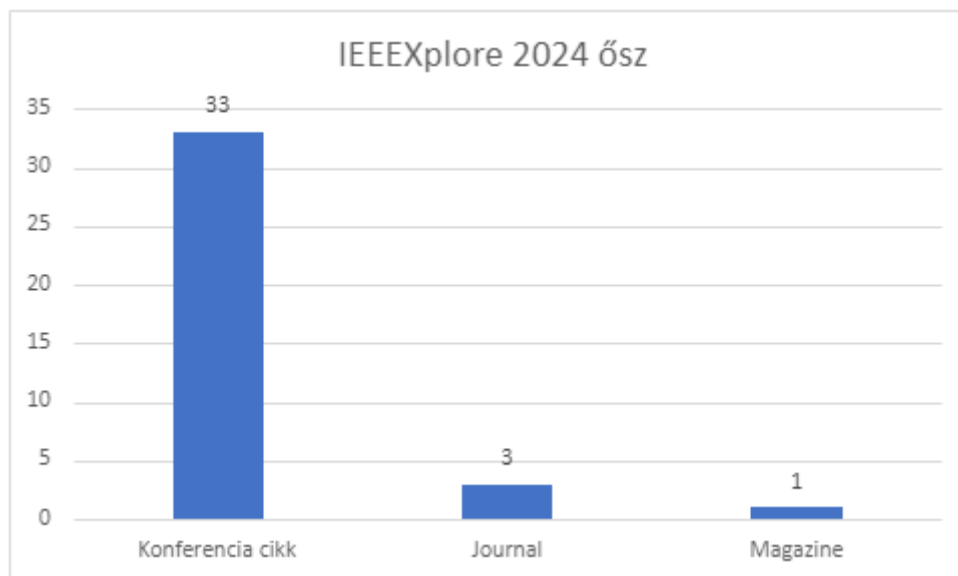
### 5.9. TUDOMÁNYREPREZENTÁCIÓ IEEEEXPLORE-BAN 2024 TAVASZ

2024 áprilisában szintén megvizsgáltam a téma reprezentációját az IEEE Xplore adatbázisban. Az előző kereséssel equiválensen mind a három kifejezést tartalmazó keresést indítottam a fejlett keresési módban (advanced search: ("All Metadata":Social Engineering) AND ("All Metadata":Email security) AND ("All Metadata":Deep Learning)) melynek sorn 36 találatot kaptam. Ezen keresés alapján nem született több IEEEExploreban indexelt tudományos közlemény. Véleményem szerint az ilyen jellegű kutatások több időt vesznek igénybe, emiatt vélhetően ősszel már növekedni fog ez a szám. [23]



### 5.10. TUDOMÁNYREPREZENTÁCIÓ IEEEEXPLORE-BAN 2024 ŐSZ

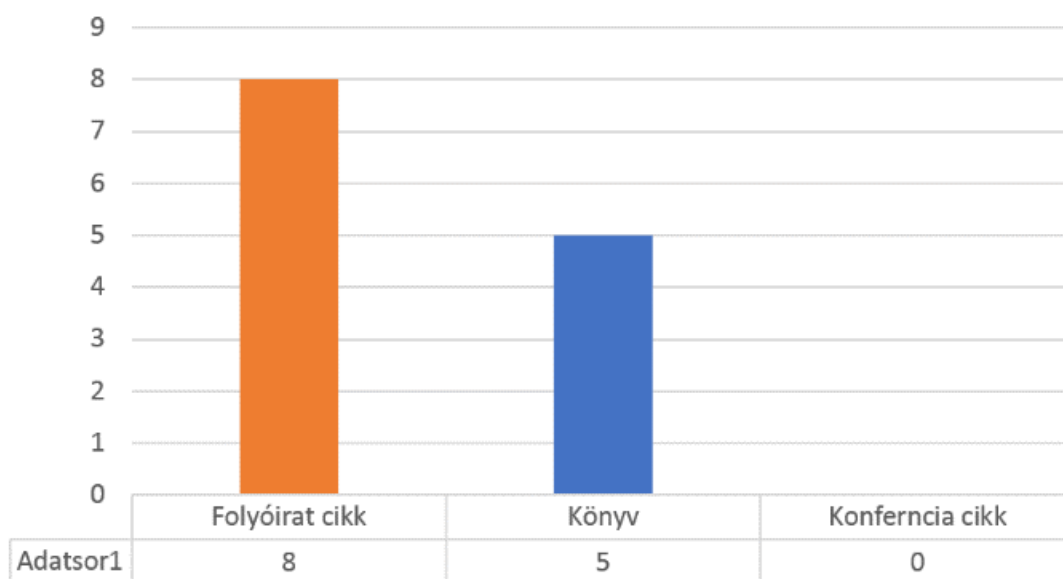
2024 novemberében szintén megvizsgáltam a téma reprezentációját az IEEE Xplore adatbázisban. Az előző kereséssel equivalensen mind a három kifejezést tartalmazó keresést indítottam a fejlett keresési módban (advanced search: ("All Metadata":Social Engineering) AND ("All Metadata":Email security) AND ("All Metadata":Deep Learning)) melynek során 37 találatot kaptam. Ezen keresés alapján nem született relevánsan több IEEEExploreban indexelt tudományos közlemény.



### 5.11. TUDOMÁNYREPREZENTÁCIÓ JSTORE-BAN 2023 ŐSZ

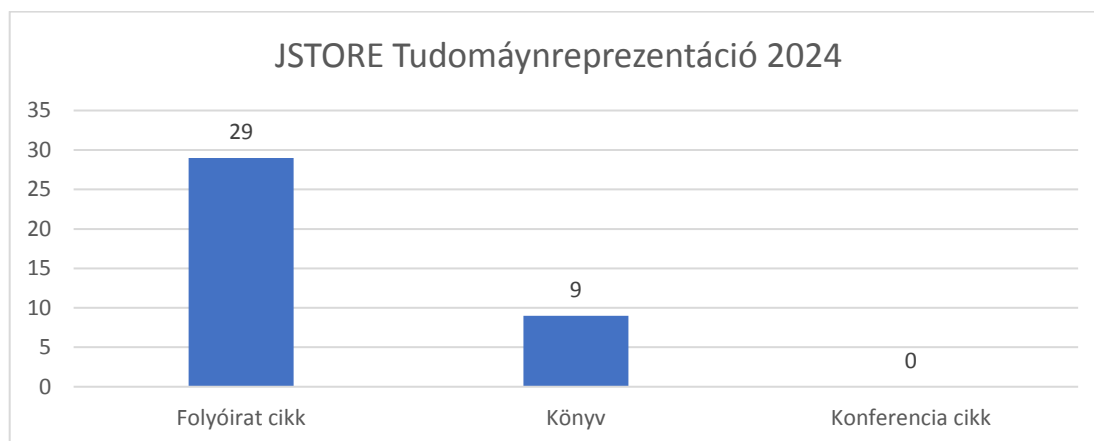
2023 novemberben tudományreprezentációt megvizsgáltam a Journal Storage (JSTORE) adatbázisban is. Itt is a fejlett keresési módban az előzőekben leírt 3 kifejezésre (Social Engineering + email security + deep learning) rákeresve a grafikonon szereplő adatokat kaptam[23]

### JSTORE tudományrepresentáció 2023 november



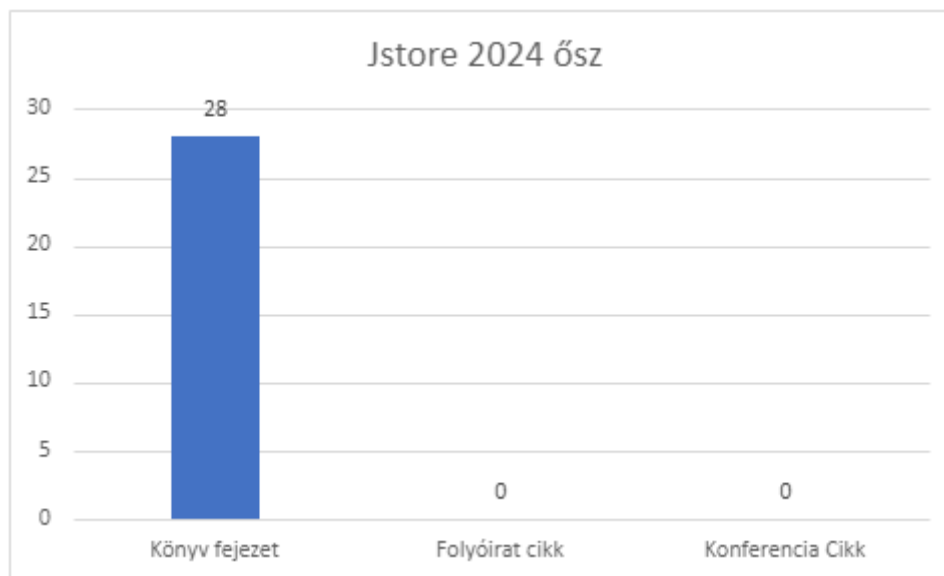
### 5.12. TUDOMÁNYREPRESENTÁCIÓ JSTORE-BAN 2024 TAVASZ

2024 áprilisában újra elvégeztem a tudományrepresentációt, ahol félév alatt néggyel több könyvben van ezzel kapcsolatos alfejezet. Valamint 21-gyel több folyóirat cikkben szerepelnek a fent leírt keresési kulcsszavak. [23]



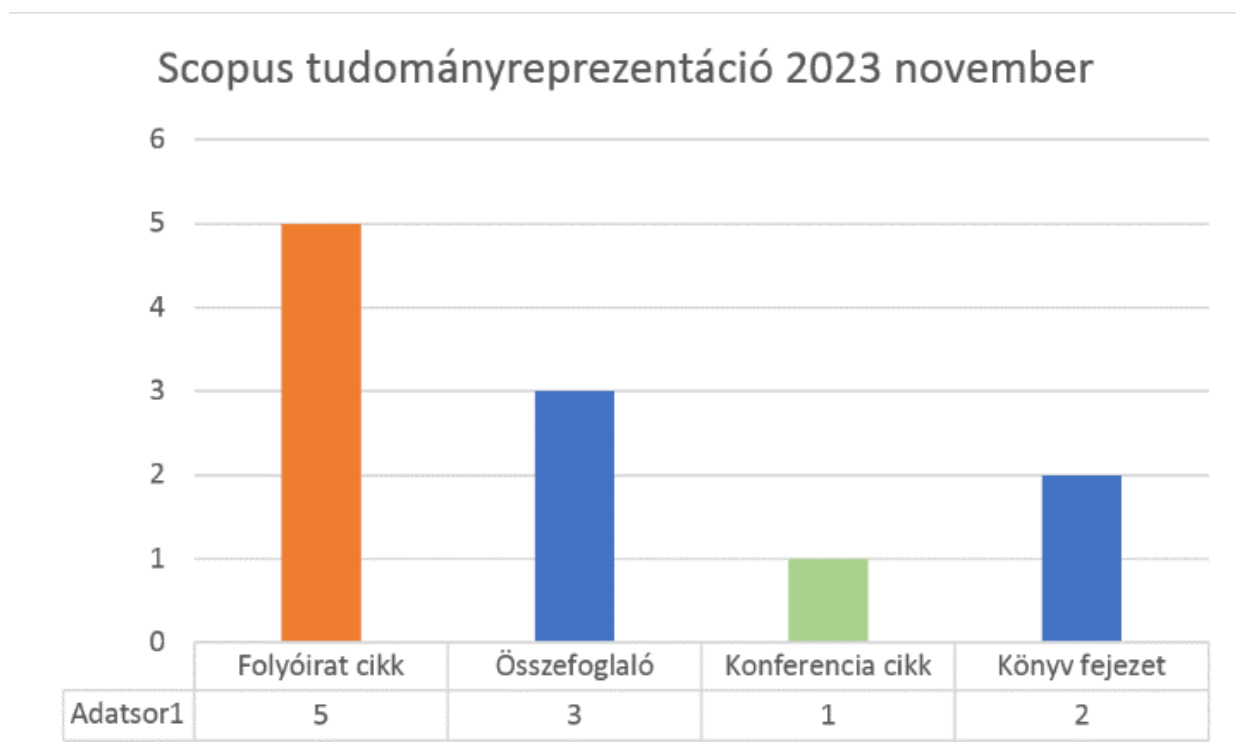
### 5.13. TUDOMÁNYREPREZENTÁCIÓ JSTORE-BAN 2024 ŐSZ

2024 novemberében újra elvégeztem a tudományreprezentációt. Ami egy furcsa eredményt adott, mivel ugyanolyan módszerrel használtam a kereső eszközöket, mint az előző félévben, de kevesebb találatot adott. Véleményem szerint ez azért lehet, mert módosítás történt a kereső motorjukban és emiatt más rekordokat hozott ki. Így ebből nem vonnék konklúziót és kizárnám ezt az eredményt a további elemzésekből.



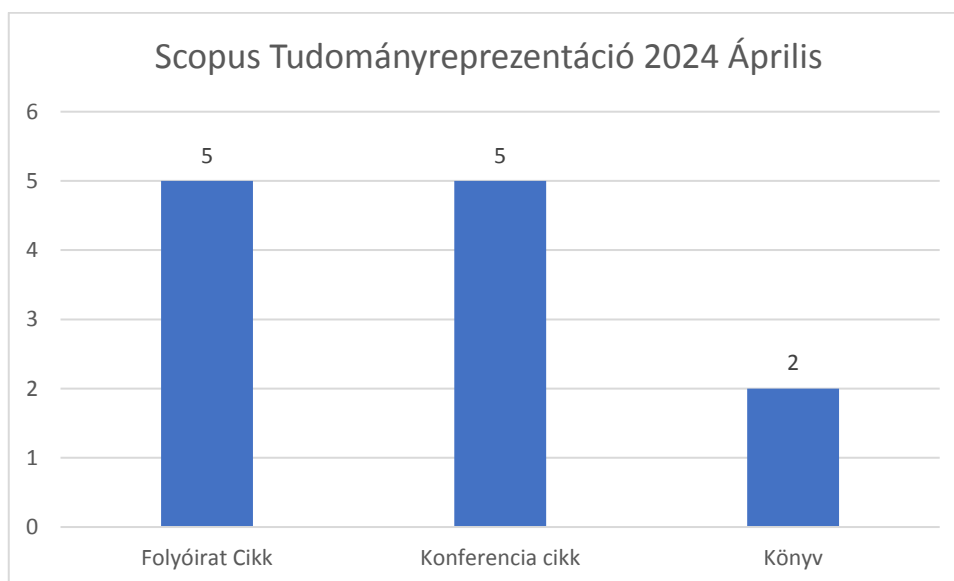
### 5.14. TUDOMÁNYREPREZENTÁCIÓ SCOPUS-BAN 2023 ŐSZ

2023 novemberében megvizsgáltam a téma tudományreprezentációját az Elsevier Scopus adatbázisában is. Itt a fejlett keresési módban az alábbi lekérdezést írtam: „ALL ( "Social Engineering" ) AND ALL ( "Email security" ) AND ALL ( deep AND learning ) AND ( LIMIT-TO ( SUBJAREA , "COMP" ) ). „ Itt is hasonlóan a JSTORE-os lekérdezéshez a „Computer Science” az az a számítás vagy számítógépes tudomány területre szűrtünk, mivel szűrés nélkül sok fals találatot kaptunk. A lekérdezés 5 folyóirat cikket, 3 tudományos összefoglalót/áttekintést, 1 konferencia cikket és 2 könyv fejezetet. [23]



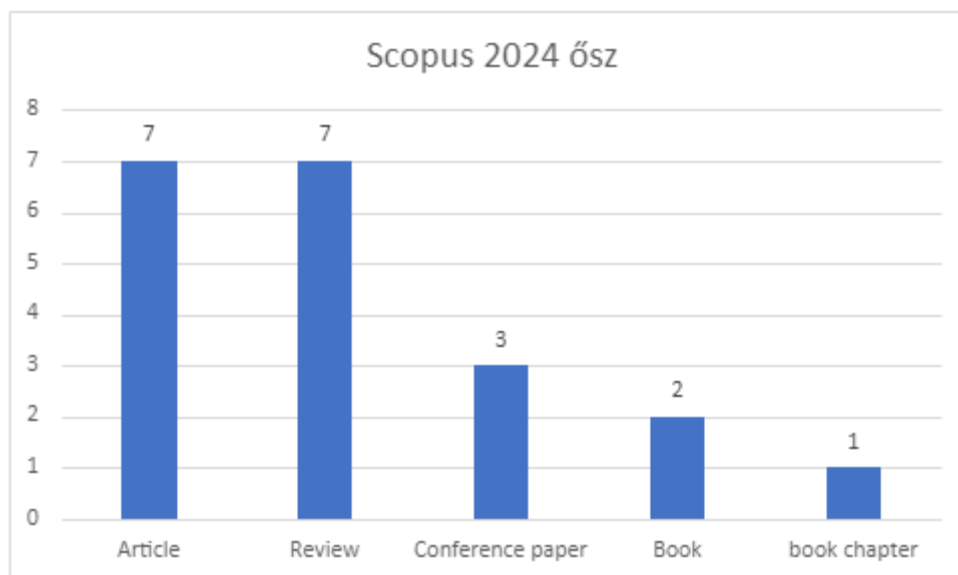
#### 5.15. TUDOMÁNYREPRESENTÁCIÓ SCOPUS-BAN 2024 TAVASZ

2024 áprilisában megismételtem a tudományrepresentációt a Scopus adatbázisában, ahol 11 helyett 12 találatot kaptam az előző félévhez képest. Ugyanakkor, ugyanazzal a search stringgel, változtak a kategóriális besorolások. Az alábbi representációból azt a konklúziót tudom levonni, hogy elhanyagolható mértékben emelkedett ebben az adatbázisban a tudományos művek száma. [23]



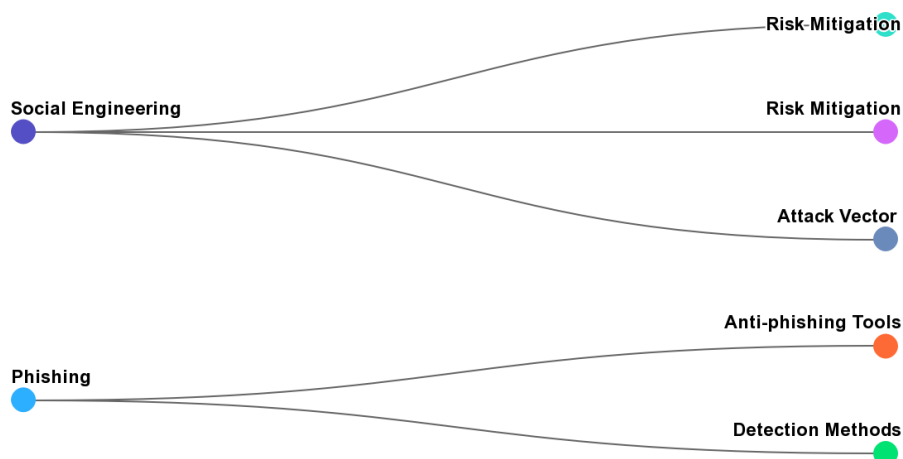
## 5.16. TUDOMÁNYREPREZENTÁCIÓ SCOPUS-BAN 2024 TAVASZ

2024 Novemberében megismételtem a tudományreprezentációt a Scopus adatbázisában, ahol 12 helyett 20 találatot kaptam az előző félévhez képest. Ugyanakkor, ugyanazzal a search stringgel, változtak a kategóriális besorolások. Az alábbi reprezentációból azt a konklúziót tudom levonni, hogy nagy relevánsan emelkedett a tudományos művek száma a scopus adatbázisban. [23]



## 5.17. SCOPUS AI – TÉMA FELDERÍTÉSE

„A Scopus béta verziójú mesterséges intelligencia téma felderítőjével is elkészítettem egy grafikont amivel gráfok segítségével láthatóvá tettük, hogy hogyan kapcsolódnak a cikkek tématerületei.” [23]

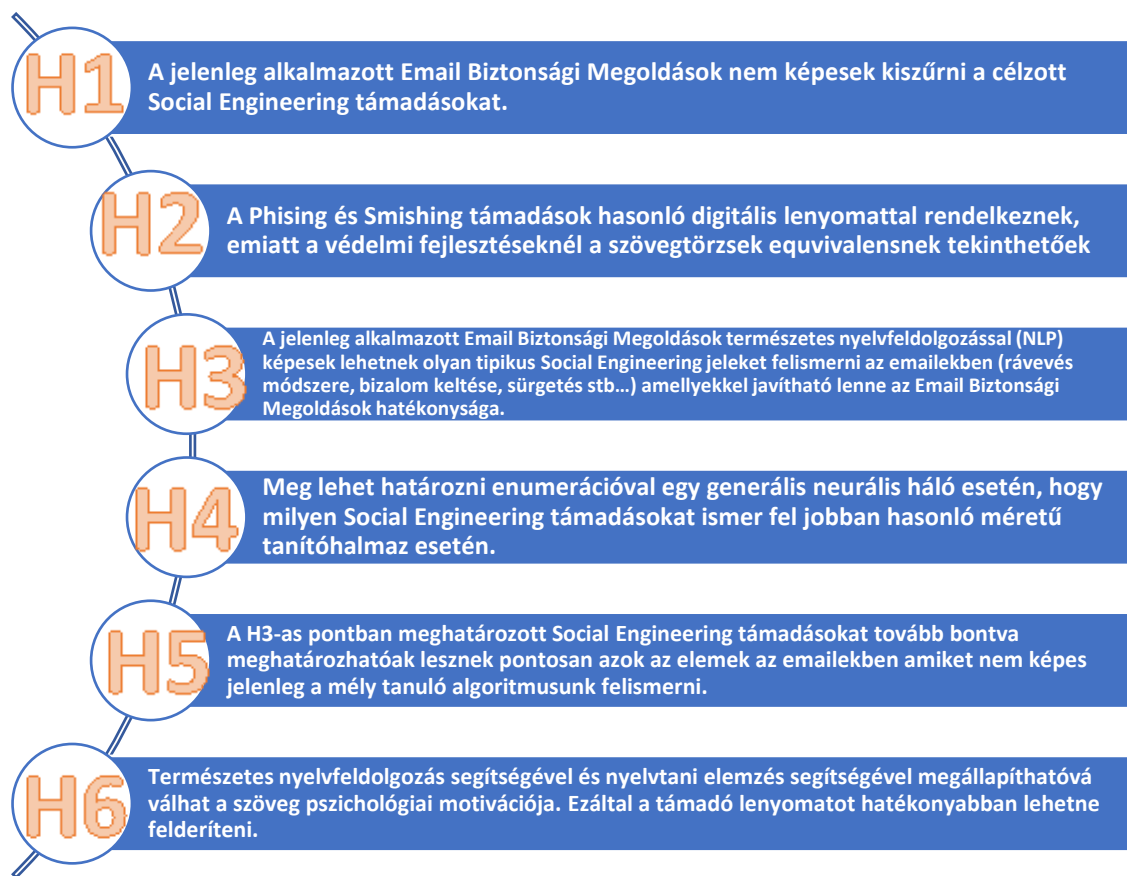


## **6. PROBLÉMÁK MEGFOGALMAZÁSA**

### **6.1. PROBLÉMA MEGFOGALMAZÁSA**

„Nagyon sok olyan műszaki/informatikai megoldással találkoztam, amik nem voltak képesek megfelelő hatékonysággal vagy egyáltalán detektálni és reagálni a Social Engineering támadásokra. Pedig, ha belegondolunk egy támadó által küldött kártékony emailt sok helyen meg lehetne fogni típustól függően. Példaképpen ki is próbáltam egy átlagos védelemmel rendelkező üzleti laptopra (reaktív vírusirtó, tűzfal, Email Biztonsági Megoldás a levelező szerver előtt) egy kártékony emailt küldeni és meglepődve tapasztaltam, hogy semmilyen riasztás nem jelzett. Továbbá nagy problémának érzem azt, hogy egyre nagyobb arányban alkalmaznak Social Engineering támadásokat a támadók, mivel a konvencionális támadásokra nagyrészt sikerült műszaki védelmet fejlesztenünk, de sajnos ilyen ütemben nem fejlesztettük a biztonsági tényező leggyengébb láncszemét a humán tényezőt. Ugyanakkor előző kutatásaim és jelenlegi interjúim rávilágítottak arra, hogy nagyon nehéz felkészíteni a munkavállalókat az ellenük professzionális szinten kidolgozott támadásokra, mikor a biztonságtudatosító képzés sokszor egy kimondottan hatékony tűz és munkavédelmi előadás hatékonyságára hajaz. Ezeket persze lehet javítani különböző módszerekkel pl.: gamifikációval [8]. A módszerek közül külön kiemelném Oroszi Eszter Diána biztonságtudatossági szabadulószoa megoldását, amivel sokkal hatékonyabban lehet ezen képzéseket elvégezni. Ugyanakkor mivel még mindig az embereket érintő tényezőről van szó, amit nehéz és költséges kezelni, ezért általánosan elmondható, hogy a szervezetek vezetői jobban örülnének olyan műszaki megoldásnak, amit egyszer megvesznek és utána egyáltalán nem, vagy csak kevesebb képzésre kell a munkavállalóit elküldenie.” [23]

## 6.2. HIPOTÉZISEK

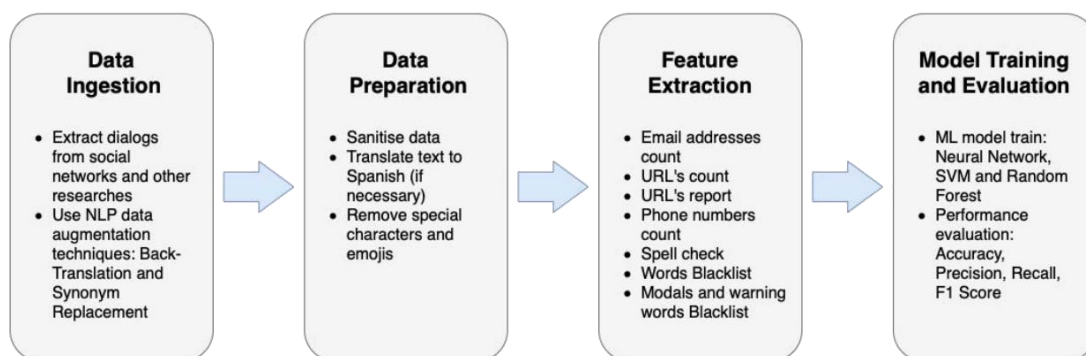


10. ábra Hipotéziseim grafikonja [23]

## 7. SZEKUNDER KUTATÁS

### 7.1. IRODALOMKUTATÁS EREDMÉNYEI

„Juan C. Lopez és Jorge E. Camargo [14] modellje NLP-t, gépi tanulást, vektoros gép segítést és véletlenszerű erdő algoritmust alkalmaz. Ezzel állításuk szerint 84%-os pontosságot tudtak elérni. A rendszerük grafikusan a következő képpen néz ki:” [23]



4. ábra [14, p 178, fig1]

„Ennél a modellnél nagyon előre mutatónak érzem, hogy NLP-vel már bizonyos Social Engineering támadási formákat már képes felismerni, mint pl.: ráhatás, túlterhelés és a tekintély bizonyos fajtáit. [14, p 179] Ezen felül a konvencionális eszköztárból is használtak URL vizsgálatot, szó fekete listát és telefonszám vizsgálatot.” [23]

„Bronjon Gogoi és Tasiruddin Ahmed [15, p 2] modellje transfer learning-et alkalmaz annak érdekében, hogy kevesebb adatból is képes legyen pontosabb döntéseket hozni. A modell alapjául a Google által fejlesztett BERT (Bidirectional Encoder Representation from Transformers) és DISTILBERT modelleket használták, mivel ezekre nagy előre tanított corpusok voltak elérhetőek. Használtak továbbá NLP-t, amit NSP-vel (Next Sentence Prediction – Következő Mondat Jóslása) és NER (Named Entity Recognition - Nevezett Entitás Felismerésel).” [23]

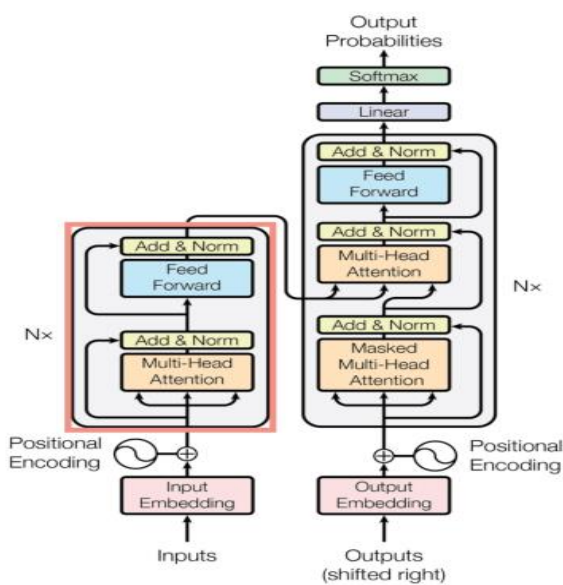


Fig. 3. Transformer Architecture

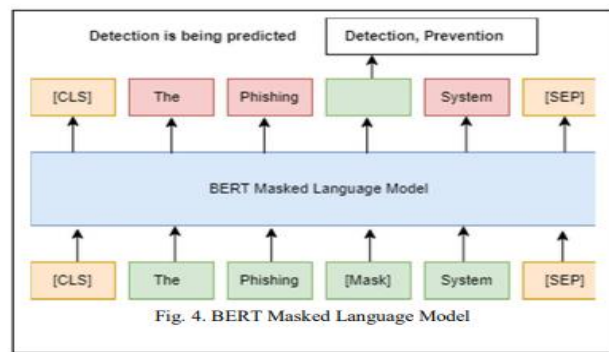


Fig. 4. BERT Masked Language Model

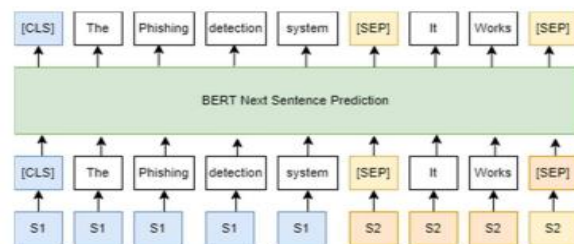


Fig. 5. BERT Next Sentence Prediction Model

11. ábra Architektúrális tervezés [28, p.3]

Egy Indiai kutatás azt vizsgálta hogyan lehet az URL-eket és az emailben lévő QR kódokat gépi és mély tanulással érzékelni. Kutatásuk hatékonysága az URL és QR kód vizsgálat során átlagosan 90% felett volt [15] [23]

Szintén Indiai kutatók egy Konvolúciós neurális hálót tanítottak fel és véletlenszerű erdő algoritmust használtak a hatékonyság növelése érdekében [16] [23]

Török kutatók SMS és Email spameket (bináris klasszifikációt használva csak 2 részre osztották a halmazt: SPAM és Nem SPAM) kiszűrő modellt készítettek, amivel magas hatékonyságot értek el, de Ők is csak 5000 alatti adathalmazt használtak. [17] [23]

Pakisztáni kutatók szintén megállapították, hogy az eddigi megoldások nagy része csak az URL-t vizsgálja és nem magát a törzs szöveget. [18] [23]

Kínai kutatók egy LSTM (hosszú rövid távú memória) és extrém gradiens támogató fa alapú megoldást dolgoztak ki az adathalász támadások ellen. 500.000-es corpusszal dolgoztak amit a CMU-CERT-től kaptak. Jelenlegi prototípusuk megfelelő alapként szolgál a további kutatásaikhoz amit folytatni fognak. [19] [23]

## 8. PRIMER KUTATÁS

### 8.1. SZAKÉRTŐI MEGKÉRDEZÉSEK

„A készített interjúk első része inkább a témám irányát határozta meg, a második része pedig olyan kihívásokat vetett fel, amik jelenleg még nem megoldottak. Az egyik leghasznosabb interjút egy telekommunikációs - szolgáltató cég üzletágvezetőjével sikerült készítenem, ahol betekintést kaphattam a telefonszolgáltatások biztonsági architektúrájába. Ezen interjú alkalmával rákérdeztem arra is, hogy az 1. ábrában említett pl.: Netflixes csalások ellen milyen védekezési mechanizmusokat használnak és mi az oka, hogy ennyire elterjedtek az SMS-es adathalás támadások. Azt a meglepő választ kapta, hogy két védekezési mechanizmust használ a szervezete (ugyanakkor kiemelte, hogy nem csak ők, hanem a többi Magyarországi szolgáltató is). Az első egy olyan empirikus predikció, amely gyanúsán sok kiküldött SMS esetén beriaszt és jelzi a szolgáltatónak, hogy pl.: 500.000 SMS-t küldtek ki ugyanazzal a szöveggel. A másik védelmi mechanizmus SMS-ek szűrésére az a jelentés alapú telefonszám kitiltás. Ez esetben, amikor kellő számú bejelentés érkezik a szolgáltatóhoz és kivizsgálják a gyanús eseteket akkor ideiglenesen letilthatják a telefonszám SMS küldési lehetőségét a hálózatról. Ezen túl viszont mást nem alkalmaznak. Ezzel a szolgáltatások biztonságát érintő megosztott felelősségi modell szerint 2 több felelősség helyeznek a felhasználóra mind a lakossági ügyfelek, mind a vállalatok esetén. Amennyiben viszont a vállalatoknál nincs megfelelő hatékonyságú biztonságtudatosító képzés ezeket a támadásokat nagy eséllyel nem fogják tudni kivédeni.

A többi interjú tartalma és eredménye megegyezett. Interjú alanyaikkal email biztonságról beszélgettem és minden interjún azt az eredményt kaptam vissza, hogy a phishing emaileket sehogyan nem tudják megfelelően szűrni. Egy alkalommal merült fel, hogy megoldás lehet, ha az email szabályzatban letiltjuk a szervezeten kívüli emailek fogadását ezzel tovább erősítve a Zero Trust<sup>3</sup> megközelítést, de ez csak kevés helyen vitelezhető ki, mivel a vállalatoknak nem a belső levelezésük termel majd bevételt. „[23]

---

<sup>2</sup> A megosztott felelősségi modell (angolul: Shared Responsibility Modell) a felhő biztonságban elterjedt biztonsági kifejezés, de véleményem szerint más kiberbiztonsági területeken is remekül használható különböző kockázati tényezőinek felírására a sok tényezős biztonsági kihívások elemzésére. [9]

<sup>3</sup> Bizalmatlanság elve. Egy olyan kiberbiztonsági jó gyakorlat a jogosultság kezelésénél, amivel csak az kap jogosultságot az adott folyamathoz vagy erőforráshoz, akinek feltétlenül szüksége van rá. Ezzel megelőzhetővé válik, hogy a fertőzés a szervezeten belül elterjedjen, illetve a visszaélések is visszaszoríthatóak vele.

## 8.2. SZAKÉRTŐI INTERJÚK EREDMÉNYEI

„A készített interjúk két fő részre oszthatók. Az első rész során a témakörrel kapcsolatos irányvonalak és kihívások kerültek felszínre, amelyek jelenleg még nincsenek teljesen megoldva. Ebben a vonatkozásban kiemelkedő interjúm volt egy telekommunikációs szolgáltató cég üzletágvezetőjével, akit Kollár Csaba 2018-as [29] cikke alapján szakértőnek lehet tekinteni, hiszen ezt foglalkozása és tapasztalata igazolja. Az interjú során az alany részletesen kifejtette a telefonszolgáltatások biztonsági architektúráját és azzal kapcsolatos védekezési mechanizmusokat. A szervezete tehát két fő védelmi mechanizmust alkalmaz. Az egyik az empirikus predikció, ami gyanúsan nagy mennyiségű SMS esetén riadót vált ki, figyelmeztetve a szolgáltatót, ha például ugyanazzal a szöveggel nagy mennyiségű SMS-t küldenek. A másik védelmi mechanizmus a jelentés alapú telefonszám kitiltás, ami akkor aktiválódik, ha a felhasználók jelentik a gyanús tevékenységet, és a szolgáltató vizsgálja a jelentéseket. Ebben az esetben ideiglenesen letilthatják a telefonszám SMS küldési lehetőségét a hálózaton. Tehát több felelősséget helyeznek a felhasználóra, mind a lakossági ügyfelek, mind a vállalatok esetén. Amennyiben viszont a felhasználó tájékozatlan, vagy nincs kiképezve ilyen üzenetek szűrésére, ezt meglehetősen bizonytalan kimenetelű módszernek találok. [23]”

Más interjúk tartalmilag hasonló eredményeket hoztak. Az emailbiztonságról folytatott beszélgetések során minden interjúalany azt emelte ki, hogy a phishing emaileket még mindig nehéz megfelelően szűrni. Egyik esetben felvetődött az ötlet, hogy az email szabályzatban a szervezeten kívüli emailek fogadását le kell tiltani, ami tovább erősítheti a Zero Trust megközelítést. Azonban ez a megoldás csak néhány helyen alkalmazható, mivel sok vállalat számára az olyan emailek is fontosak lehetnek, amelyek a vállalaton kívülről érkeznek, és az ilyen tiltás az üzleti tevékenységet is negatívan befolyásolhatja, mivel nem minden esetben a belső levelezés generálja a bevételeket [23]

A szakértői interjúk során azt a konklúziót vontam le, hogy a téma aktuális, megéri vele foglalkozni, mivel nem állnak rendelkezésre megfelelő gyakorlatok sem az iparban, sem az állami szférában. [23]

### 8.3. LAKOSSÁGI MEGKÉRDEZÉS (KÉRDŐÍVVEL)

#### 8.3.1. Módszertan

A kutatás célja az adathalászat jelenségének társadalmi hatásainak feltárása, az áldozatok és környezetük tapasztalatainak vizsgálata, valamint az érintettség mértékének és az emberek hozzáállásának felmérése Magyarországon. A kutatás során egy kérdőíves módszert alkalmaztam, amelyet online platformon keresztül juttattam el a válaszadókhoz.

##### 8.3.1.1. A kérdőíves kutatás típusa és célja

A kutatás kvantitatív jellegű volt, amely lehetővé tette, hogy statisztikailag elemezhető adatokat gyűjtsen az adathalászattal kapcsolatos ismeretekről, személyes és közvetlen tapasztalatokról, valamint a téma megítéléséről. A kérdőívet úgy terveztem, hogy a célcsoport széles spektrumát lefedje a nem, kor és végzettség szempontjából, lehetővé téve a különböző demográfiai csoportok közötti különbségek és hasonlóságok vizsgálatát.

##### 8.3.1.2. Mintavételi eljárás

A kérdőívet online platformokon tettem elérhetővé (pl. közösségi média csoportok, szakmai fórumok, hírlevelek). Az online elérés lehetővé tette, hogy széleskörűen, földrajzi korlátozások nélkül gyűjtsen válaszokat, ezáltal növelve a minta sokszínűségét. A mintavétel nem-probabilista, önkéntes alapú, amely lehetővé tette a kutatásban való részvételt azok számára, akik érdeklődést mutattak a téma iránt, és nyitottak voltak a válaszadásra.

##### 8.3.1.3. A kérdőív felépítése

A kérdőív összesen 12 kérdést tartalmazott, amelyek zárt és félig nyitott kérdések formájában kerültek megfogalmazásra. A kérdéseket több csoportba rendeztük a következők szerint:

**Demográfiai jellemzők:** Itt a válaszadó nemére, korára és végzettségére vonatkozó információkat gyűjtöttünk. Ezek az adatok fontosak az elemzésekhez, mert lehetővé teszik a válaszok szegmentálását és a demográfiai változók hatásának vizsgálatát.

Ismeret és tapasztalat az adathalászat terén: A következő kérdések az adathalászat fogalmának ismeretére (hallott-e már róla) és az ezzel kapcsolatos saját vagy közvetlen tapasztalatokra vonatkoztak, például hogy a válaszadó próbálták-e már ilyen módon becsapni, illetve esett-e már maga is áldozatul.

**Környezet érintettsége:** Ebben a szekcióban a válaszadót arra kértük, hogy nyilatkozzon arról, tud-e bárkiről a környezetében, aki adathalászat áldozata lett, és ha igen, hány személyről van tudomása.

**Kárfelmérés és típuselemzés:** Kérdéseink kitértek arra is, hogy a válaszadó vagy környezetében mások milyen kárt szenvedtek el az esetleges adathalász támadások következtében, valamint, hogy milyen típusú adathalászatot tapasztaltak vagy hallottak.

Nyílt kérdés a válaszadók meglátásairól: Végezetül egy félig nyitott kérdésben lehetőséget biztosítottunk arra, hogy a válaszadók megosszák bármely további észrevételüket vagy személyes véleményüket a témával kapcsolatban.

#### **8.3.1.4. Kutatási korlátok**

Az önkéntes válaszadás önszelekciós hatása is torzíthatta az eredményeket, mivel valószínűleg nagyobb arányban válaszoltak azok, akiket valamilyen szinten már érintett a probléma.

Valamint fontosnak tartom kiemelni, hogy a 132 válaszadó nem reprezentatív kérdőíves kutatás és nem tekinthető pusztán statisztikailag reprezentatívnak, ugyanakkor fontos volt számomra ennek az elkészítése, mivel azt kívántam vizsgálni vele (ami alátámasztást is nyert), hogy az én személyes környezetemet mennyire érinti.

Az összességében elmondható, hogy a Magyarországon élő kb 800.000 18-25 éves korosztályhoz viszonyítva a kérdőívet 95 fő töltötte ki aki ebbe a korosztályba esett ez kevesebb mint 0,02%-a ennek a lakossági szegmensnek ezért tekinthető korlátozottan reprezentatívnak.

#### **8.3.2. Eredmények**

„Az adathalászat kérdőívet 132 válaszadó töltötte ki, akik különböző neműek és korcsoportokba tartoznak. A válaszok szerint a résztvevők többsége férfi (54.5%), de nők (39.4%) és nem-bináris (2,3%) személyek is kitöltötték a kérdőívet. További 2,3% nem kívánt válaszolni és 1,5% pedig az egyéb kategóriába sorolta magát.

A kérdőív válaszadói között széleskörű korcsoport-eloszlás figyelhető meg. A legnagyobb arányban az 18-25 év közötti korcsoport szerepelt, akik a válaszadók 72,3%-át tették ki. Ezt követték a kis- és fiatalok (13-17 év) 9,8%-kal, az 26-35 év közöttiek szintén 9,8%-kal, az 36-45 év közöttiek 4,5%-kal, az 46-55 év közöttiek 2,3%-kal, és végül az 65 év felettiek 0,8%-kal. A válaszadók között tehát széles körű korcsoportok képviseltették magukat, amelyek között az 18-25 év közöttiek domináltak, amivel teljesítettük azon célkitűzésünket, hogy a kutatásunk elsődlegesen a saját kortársainkra fókuszáljunk.

Az iskolázottság terén a fiatal felnőttek túlnyomó többsége miatt hasonlóan mérsékelt a szórás. A válaszadók között az általános iskolai végzettséggel rendelkezők 18,9%-ban képviseltették magukat. A leggyakoribb végzettség az érettségi volt, amelyet a válaszadók 31,8%-a szerzett meg. A középfokú szakirányú végzettséggel rendelkezők 18,9%-ban szerepeltek. A BA/BSc vagy főiskolai végzettséggel rendelkezők 20,4%-ot tettek ki. A felsőoktatási szakképzést 3%-

an, az MA/MSc vagy egyetemi végzettséget 3,8% szerzett. A PhD-t szerzettek 1,5%-ot képviseltek a válaszokban, míg az egyéb végzettséggel rendelkezők aránya 1,5% volt. Így az iskolázottság terén is sokféle végzettséggel rendelkező válaszadók találhatók a mintában, de az érettségivel és a BA/BSc végzettséggel rendelkezők egyértelműen dominálnak.

Az adathalászat jelensége iránti tudatosság és az áldozattá válás mértéke is fontos részét képezi a kutatásnak. A válaszadók 124-en, azaz 94.7%-a már hallott az adathalászatról, míg csak 8-en, azaz 6.1%-a nyilatkozott úgy, hogy még soha nem találkozott ezzel a kibertámadási formával. Az áldozattá válás szempontjából a válaszok szintén beszédesebbek. A válaszadók 101-en, azaz 76.5%-a mondta, hogy már próbálkoztak az adatai kicsalásával, míg 31-en, azaz 23.5%-a nyilatkozott úgy, hogy még nem volt áldozata ilyen támadásnak. Azok között, akik már áldozattá váltak, 19-en, azaz 14.4% mondta, hogy legalább egyszer esett már adathalászat áldozatául, míg a többiek szerencsésebbek voltak, és nem sétáltak bele ilyen támadásokba. A válaszok alapján tehát elmondható, hogy a megkérdezettek nagy része hallott már az adathalászat jelenségéről, tehát tudatosabbak a jelenséggel kapcsolatban, amivel gyakran találkoznak is és kevésbé esnek általa csapdába.

Ugyanakkor azok közül, akik válaszoltak a kérdésre, hogy „Tudnak-e a környezetükben olyan személyről, aki esett adathalászat áldozatául?”, a válaszok alapján a következő arányok állnak fenn: az igen válaszadók aránya 37,74%, míg a nem válaszadók 62,26%-ot képviselnek. A válaszadók között, akik igen válaszoltak, különböző mértékű áldozattá válások is előfordultak. Ebből adódóan, az 1 fő által tapasztalt esetek aránya 4,72%, a 2-5 fő közötti eseteké 27,36%, 5-10 fő közötti eseteké 4,72%, 10-25 fő közötti eseteké 2,83%, és több mint 100 fő áldozatává válás is előfordult, amelyet a válaszadók 1,89%-a jelentett. Fontos kiemelni, hogy a 25-50 fő közötti esetről és a 50-100 fő közötti esetről szóló válaszok aránya mindkét esetben 0% volt ebben a mintában. A válaszok összességében bemutatják a környezetükben esett phishing áldozatok változatos számát és gyakoriságát az adatokban.

A "Többször is megtörtént-e a támadás?" kérdésre adott válaszokat elemezve megállapítható, hogy a kitöltők különböző mértékben tapasztalták az adathalász támadásokat. A válaszok eloszlása a következőképpen alakult: 9,8% azok, akik szerint elég gyakran érték őket ilyen támadások, 37,7% pedig azt mondta, hogy néha megesik velük. Emellett 24,6% azt állította, hogy csupán egyszer érte már ilyen támadás, míg 21,3% szerint bár még nem tapasztalták, megeshetett volna velük. A válaszadók 6,6%-a úgy véli, hogy nem eshetnek áldozatul ilyen támadásoknak, és 0,0% nem kívánta megosztani adatait ezzel kapcsolatban.

A keletkezett kár értékét tekintve az elenyészőtől, a pár ezer forintos és néhány százezer, majd pár milliós károkon keresztül egészen a több száz milliós károkig számoltak be minden féléről a válaszadók szabad, szöveges válaszaikban. Volt olyan is, aki leginkább a kár helyrehozatalára szánt időt fájlalta különösen utólag.

Az adatok alapján a válaszadók közül 90.2% hallott az Email Phishing-ről (Email Adathalászat), míg a Spear Phishing (Lándzsás adathalászat+) típusról 44.7% tájékozott. A Pharming (Pharming) jelenségéről 43.9% hallott már, míg a Vishing (Hang-phishing) típusról 58.3% számolt be. A Smishing (SMS-phishing) ismertsége 73.5%, a Clone Phishing (Klónozó-phishing) pedig 49.2%. A Whaling (Nagyhalászat) jelenségről 19.7% hallott, míg a Social Media Phishing (Társadalmi médiaphishing) típusra 70.5% emlékszik. Az Üzleti e-mail meghekkelés (Business Email Compromise - BEC) típust 34.8% ismerte fel, míg a Kiberbűnözési támadások (Ransomware Attacks) típusáról 48.5% hallott.

Az összegzés során azt látjuk, hogy az adathalászat széles körű probléma, és sokféle típusú támadás érintheti az embereket. Az emberek különböző módon reagálnak az ilyen támadásokra, és vannak, akik már többször is áldozattá váltak, míg mások szerencsére elkerülték ezeket a veszélyeket, de többen környezetükben nem voltak ennyire szerencsések. Az adathalászattal kapcsolatos ismeretek terén még mindig van fejlődési lehetőség, és az embereknek fontosnak kell tartaniuk az online biztonságukat.” [23]

#### 1. Neme

[További részletek](#)

[Betekintések](#)

|                        |    |
|------------------------|----|
| Férfi                  | 78 |
| Nő                     | 54 |
| Nem-bináris            | 3  |
| Nem kívánom megosztani | 3  |
| Egyéb                  | 2  |

#### 3. Végzettség

[További részletek](#)

[Betekintések](#)

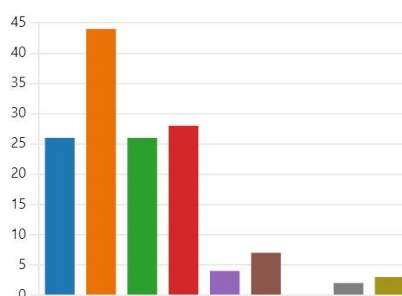
|                                  |    |
|----------------------------------|----|
| Általános iskola                 | 26 |
| Érettségi                        | 44 |
| Középfokú szakirányú végzettség  | 26 |
| BA/BSc vagy Főiskolai végzettség | 28 |
| Felsőoktatási szakképzés         | 4  |
| MA/MSc vagy Egyetemi végzett...  | 7  |
| Posztgraduális képzés            | 0  |
| Phd                              | 2  |
| Egyéb                            | 3  |

#### 2. Kora

[További részletek](#)

[Betekintések](#)

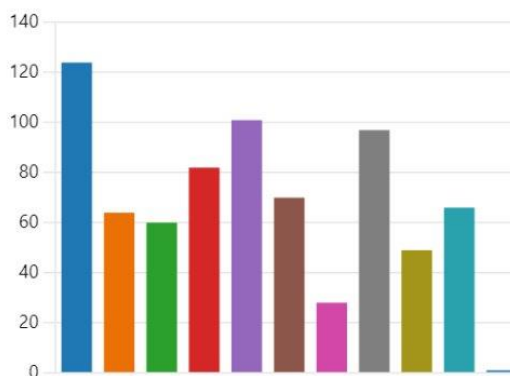
|                  |     |
|------------------|-----|
| Kis-, fiatalkorú | 13  |
| 18-25            | 103 |
| 26-35            | 14  |
| 36-45            | 6   |
| 46-55            | 3   |
| 56-65            | 0   |
| 65+              | 1   |



## 11. Milyen típusú phishingről hallott már vagy találkozott vele?

[További részletek](#)

|                                      |     |
|--------------------------------------|-----|
| Email Phishing (Email Phishing): ... | 124 |
| Spear Phishing (Lándzsa-phishin...   | 64  |
| Pharming (Pharming): A támadó...     | 60  |
| Vishing (Hang-phishing): A vishi...  | 82  |
| Smishing (SMS-phishing): Haso...     | 101 |
| Clone Phishing (Klónozó-phishi...    | 70  |
| Whaling (Nagyhalászat): Ez a ve...   | 28  |
| Social Media Phishing (Társadal...   | 97  |
| Business Email Compromise (BE...     | 49  |
| Ransomware Attacks (Zsebpénz...      | 66  |
| Egyéb                                | 1   |



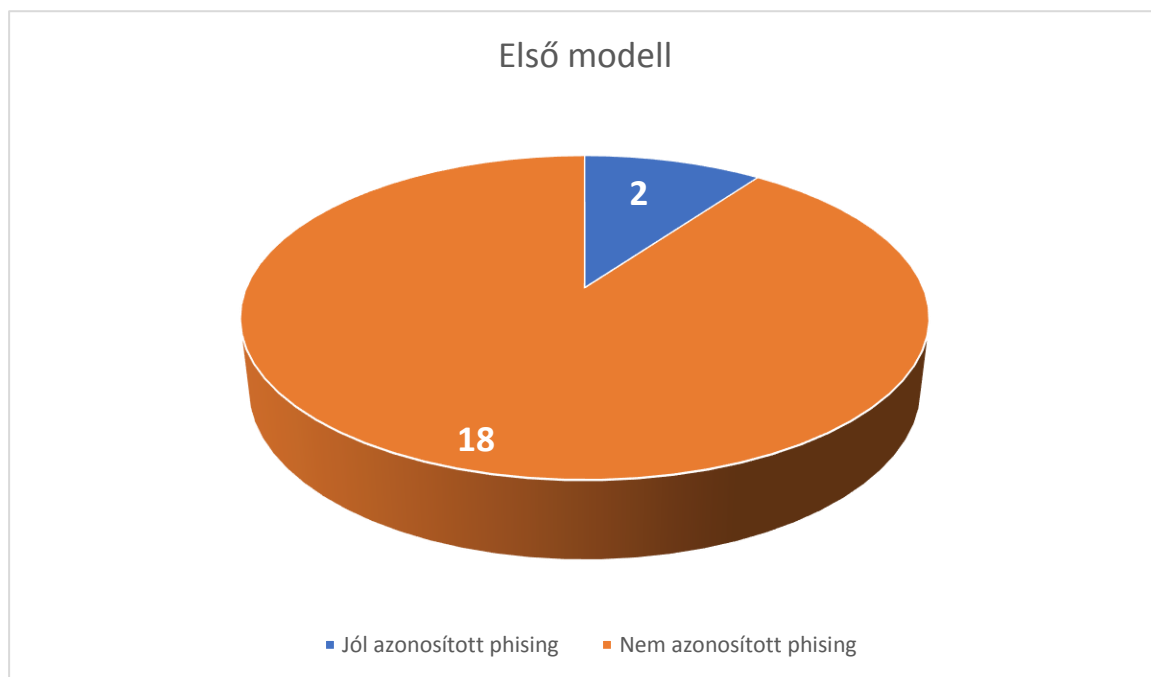
### 8.4. KORÁBBI MÉRÉSEK BEMUTATÁSA

„Sokszor futottam bele primer kutatásom során abba, hogy nagyon magas hatékonyságúnak ígérkező klasszifikáló modelleket találtam a közösség által fejlesztett Kaggle nevű oldalon. [10] Itt sokszor 90+ % hatékonyságú modelleket láttam, viszont nekem ez gyanúsnak tűnt, mivel amikor korábban készítettem egy interjút egy telekommunikációs cég kutató mérnökével, tőle azt az információt kaptam, hogy annak ellenére, hogy piacvezető beszállítók ilyen technológiában viszont 30-40%-nál nagyobb hatékonyságot nem tudtak elérni. Ebből arra következtettem, hogy ahol nagyon magas hatékonyságot látok, ott a modellt túltaníthatták, ennek következményében az eredeti adat halmazával jó eredményeket tud elérni, viszont valós támadások esetén már sokkal kevésbé.

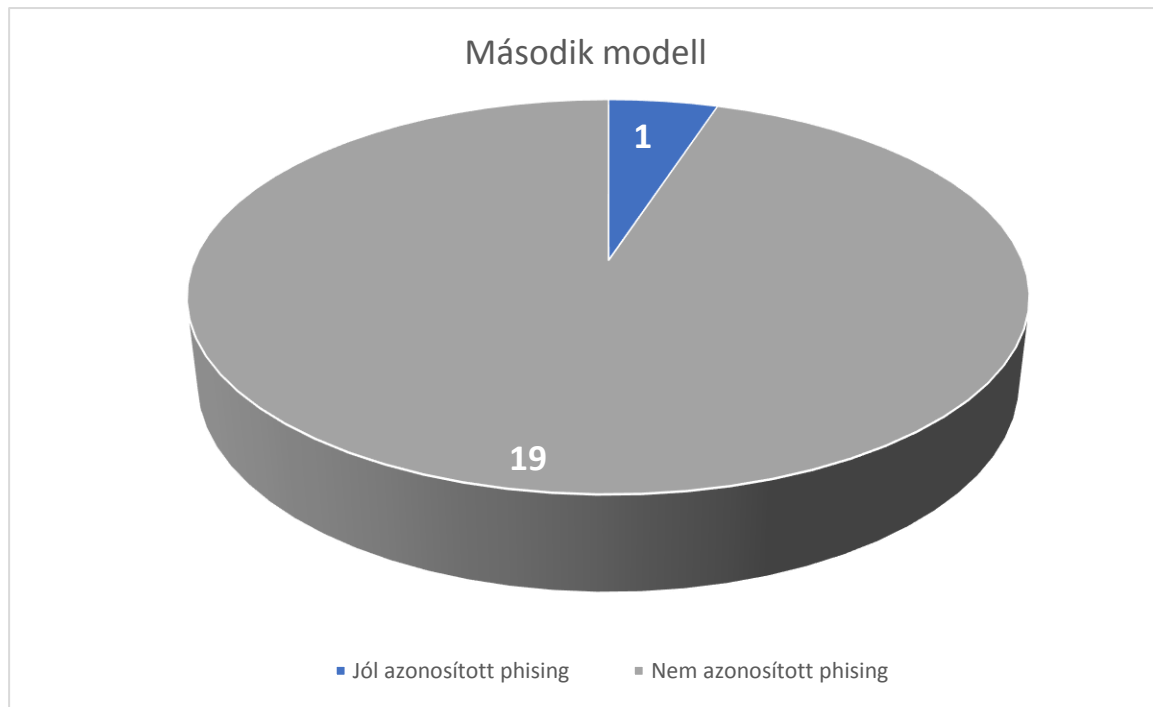
Ennek igazolására 3 modellnél [11][12][13] megmértem mi történne, ha én írnék phishing emaileket, amiket a papíron jól teljesítő modelleknek kellene klasszifikálnia. Mind három modell esetében 20-20 emaillel végeztem méréseket. Fontos azonban kiemelnem, hogy a használt modellek alapvetően binárisan foglalkoztak az email biztonsággal. Vélhetően az egyszerűség

és vagy a hatékonyság (futási időre értendő, nem pontosságra) kedvéért, de nem tesznek különbséget a SPAM, phishing vagy egyéb más kártékony emailek között. A SPAM kategóriába kerül minden kártékony email. Ezt az eredmények értékelésénél fontos figyelembe venni. Az eredményeim grafikus formában itt láthatóak:” [23]

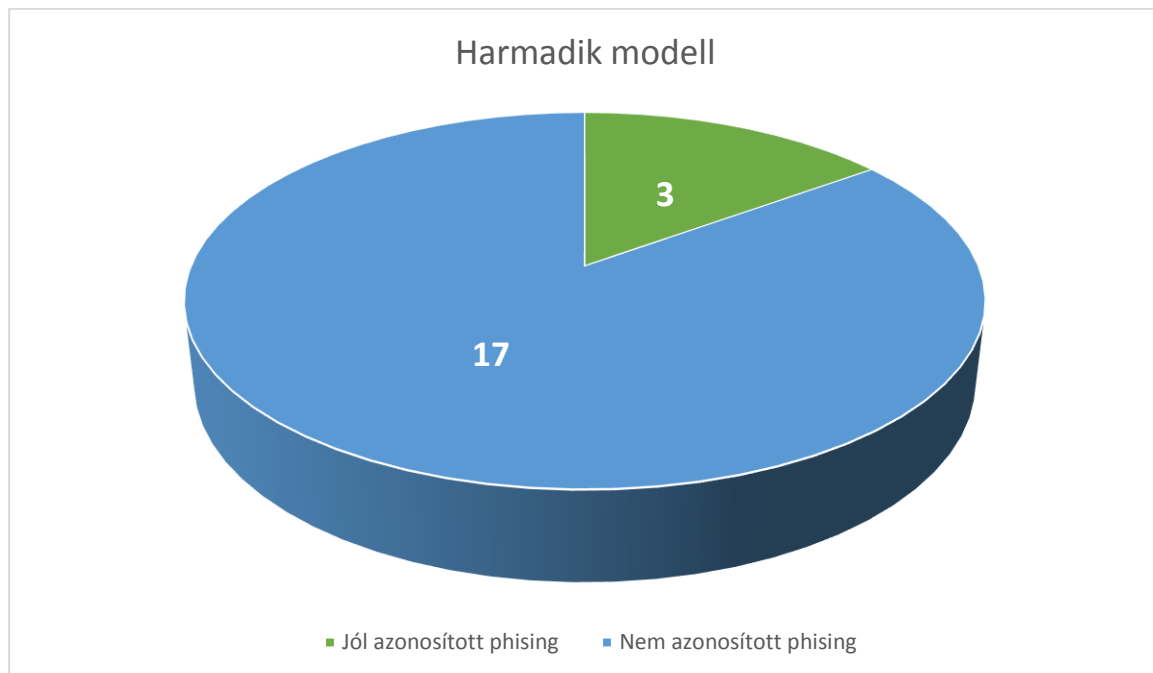
#### 8.4.1. 1. Modell



#### 8.4.2. 2. Modell



#### 8.4.3. 3. Modell



#### 8.4.4. További modellek sikertelensége

Bizonyos modellek esetén pedig a még emberek számára is feltűnően egyértelmű támadások azok amiket nem érzékelnek. Ezeknek az oka véleményen szerint az lehet, hogy nagyon kis

méretű és főleg egy típusú adathalmazból túltanították a modellt, ezáltal egy nagyon kis szegmenst nagyon jól lefed, de a támadások nagy többségét nem fogja érzékelni.

Oracle sphere test!

```
[ ] prediction_on_test_data = model.predict(X_test_features)
    accuracy_on_test_data = accuracy_score(Y_test, prediction_on_test_data)
```

```
[ ] print('Accuracy on test data: ', accuracy_on_test_data)
```

Accuracy on test data: 0.9659192825112107

Predictive System INPUT

```
[ ] input_mail = ["Won 5 free entry for the basketball match click on the link to achive: http://totallyscam.com/scam/phising/spam/thisistotallynotavirus.exe"]
    # Text --> Vector
    input_data_features = feature_extraction.transform(input_mail)

    #PRED
    prediction = model.predict(input_data_features)
    print(prediction)

    if(prediction[0] ==1):
        print('Ham Mail')

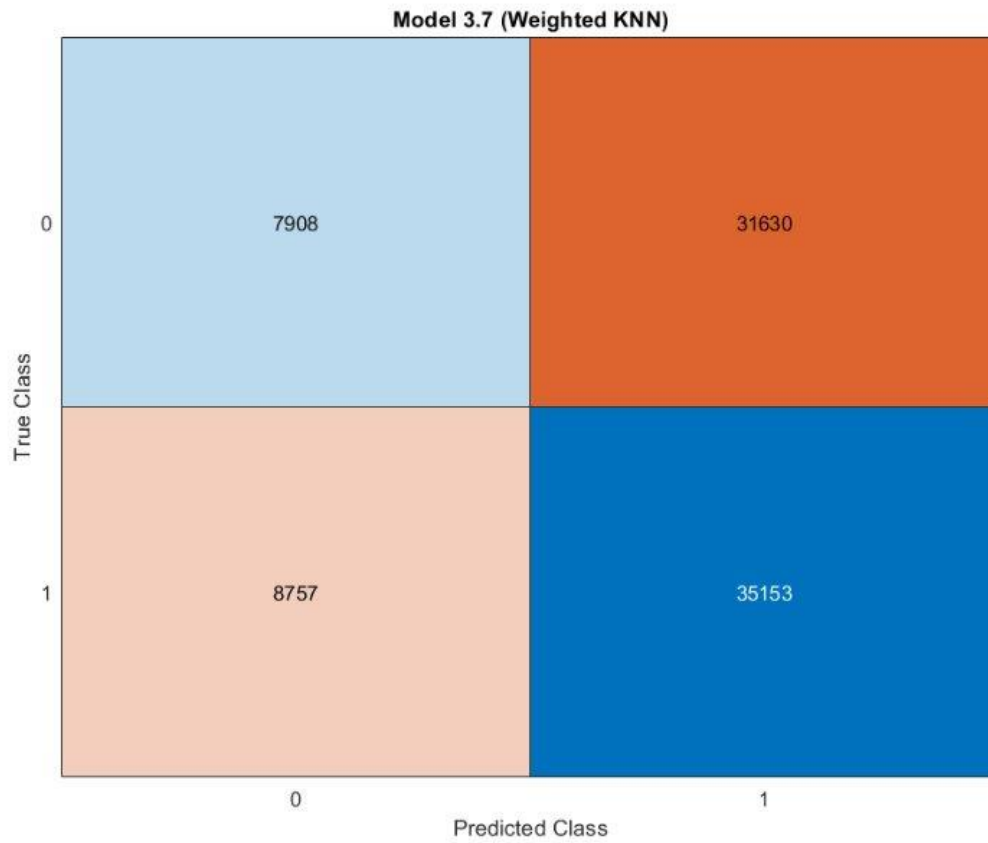
    else:
        print('Spam mail')

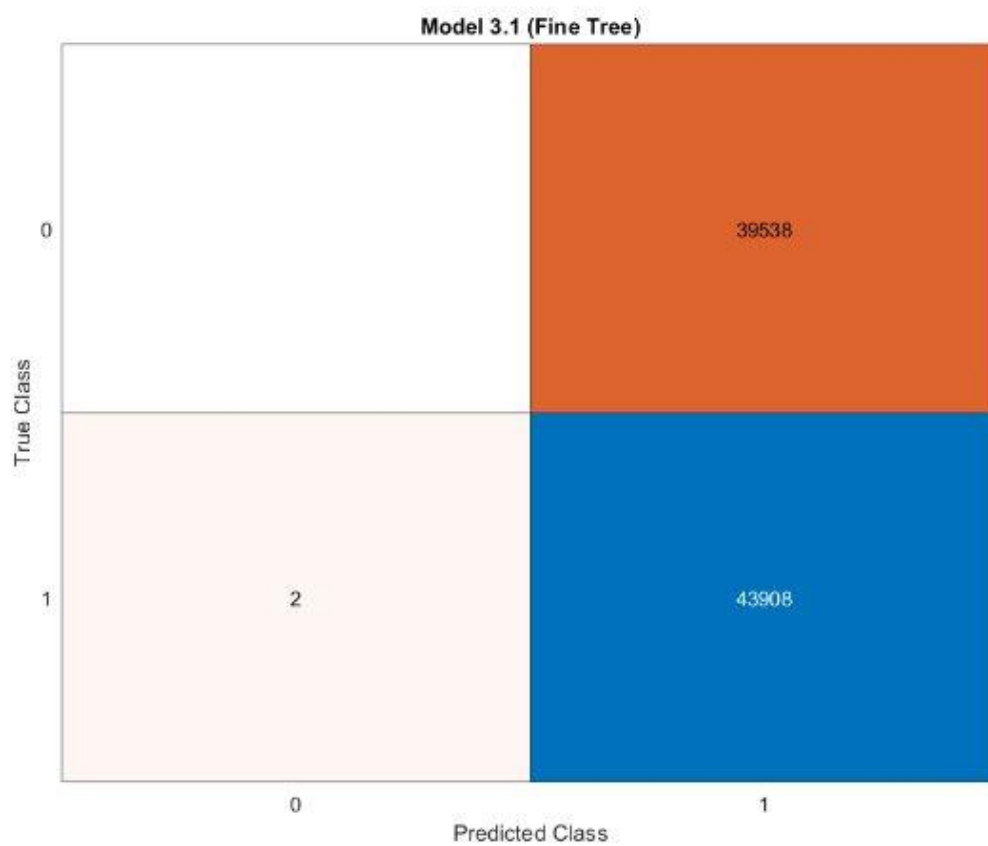
[1]
Ham Mail
```

12. ábra Szerző által fejlesztett modell és szerző által szerkesztett kép

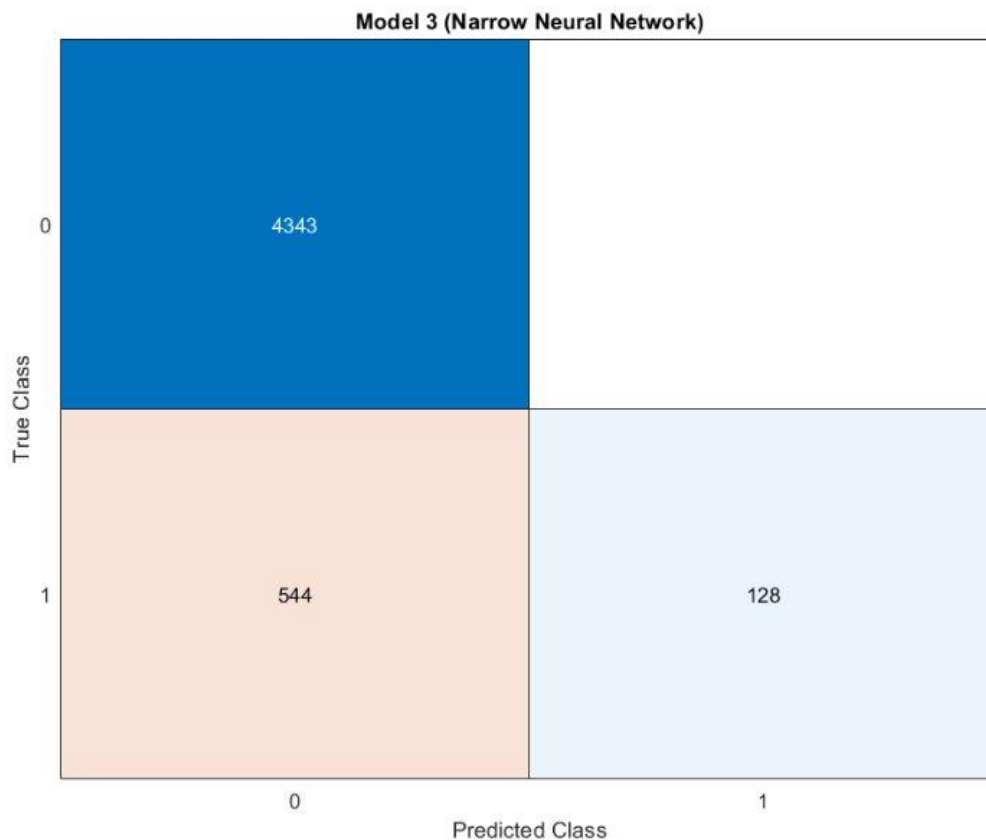
## 8.5. FRISS MÉRÉSI EREDMÉNYEK

### 8.5.1. Kártékony Emailek detektálása





### 8.5.2. Kártékony SMS-ek detektálása



### 8.6. EMAIL EXPORT-IMPORT ELŐRE PONTOZÁS

„A szakirodalom [15], valamint az iparban használatos megoldásokban [30] is bevett rendszer az, hogy előre pontozzák a kockázatot különböző tényezők alapján.

Ezt mi is megtettük. Ezért a Microsoft Office365 Outlook levelező rendszeréhez készítettünk egy Microsoft Power Automate folyamatot ami a beérkező emaileket mielőtt a felhasználó olvasná kiszedi a beérkezett email közül és elvéggez rajta olyan ellenőrzéseket amivel a nagyobb kockázati besorolásokat meg lehet tenni (ezt részletezem lentebb), majd átadja az emailt egy mély tanuló modellnek. Ezután visszakapja a Power Automate folyamat a feldolgozott emailt és a kockázati százalék alapján a rendszerüzemeltetés beállításai alapján dönt arról, hogy az email átengedhető-e vagy eldobandó.

A Power Automate folyamatunk először is megvizsgálja a küldő felet. Amennyiben saját tartományon belüli a küldő, úgy nem emeli a kockázati pontszámot, mivel a saját tartományon belülről érkező támadások nagyrészt nem adathalász alapúak. Megvizsgálja, hogy a tárgy és a

szövegtörzs tartalmaz-e gyakran alkalmazott adathalász mondatot. Valamint megvizsgálja, hogy tartalmaz-e kártékonynak tűnő csatolmányt.” [23]

## **8.7. ÚJ TÁMADÁSI OSZTÁLYOK LÉTREHOZÁSA**

Korábbi kutatásom során azt a konklúziót vontam le, hogy jelenleg a szakirodalom nem rendelkezik elég mély osztályozási rendszerrel a támadások klasszifikációja kapcsán. Ezért világossá vált, hogy amennyiben az adathalász támadásokat mély tanulás során jobban detektálhatóvá akarjuk tenni szükségünk van több osztályra, ami további tulajdonságokat jelenthet a neurális hálónk számára. Az új osztályok elkészítését elkezdtem, de mivel nagyon sok nyelvi elem is befolyásolja az új osztályok kialakítását ezért a Magyar Kiberbiztonsági Klaszter-től igényeltem email adatbázisokat kutatási célra. Ezek még nem érkeztek meg a TDK leadásának pillanatáig. Ennek mélyrehatóelemzése után előreláthatólag 2025 tavaszán kerülhetnek bemutatásra az új osztályok. [23]

## **8.8. MÉRÉSEK SZABADON HASZNÁLHATÓ NAGY NYELVI MODELLEKKEL**

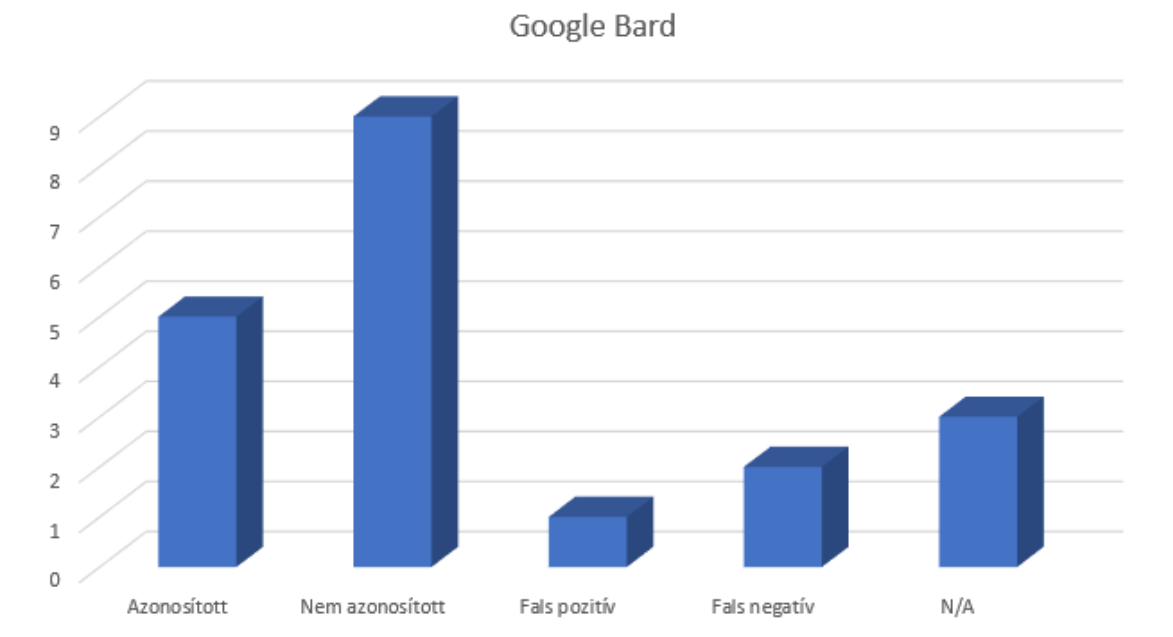
Mivel manapság nagyon felkapottak lettek az NLP alapú nagy nyelvi modellek ezért 2 ilyen modell esetén megvizsgáltuk az ilyen nagy nyelvi modellek alkalmazhatóságát. Ezt 2023 őszén végeztem amikor még a Google nem nevezte át a Bard-ot Gemininek. [23]

### **8.8.1. Bard**

„A Google által fejlesztett Bard hasonlóan a ChatGPT-hez egy nagy nyelvi modell amivel egy chat felületen képesen vagyunk interaktálni. Kutatásom során megvizsgálta, hogy egy ilyen nagy nyelvi modell amely természetes nyelvfeldolgozáson alapul képes-e segítségünkre lenni abban, hogy kiszűrjük az adathalász támadásokat.

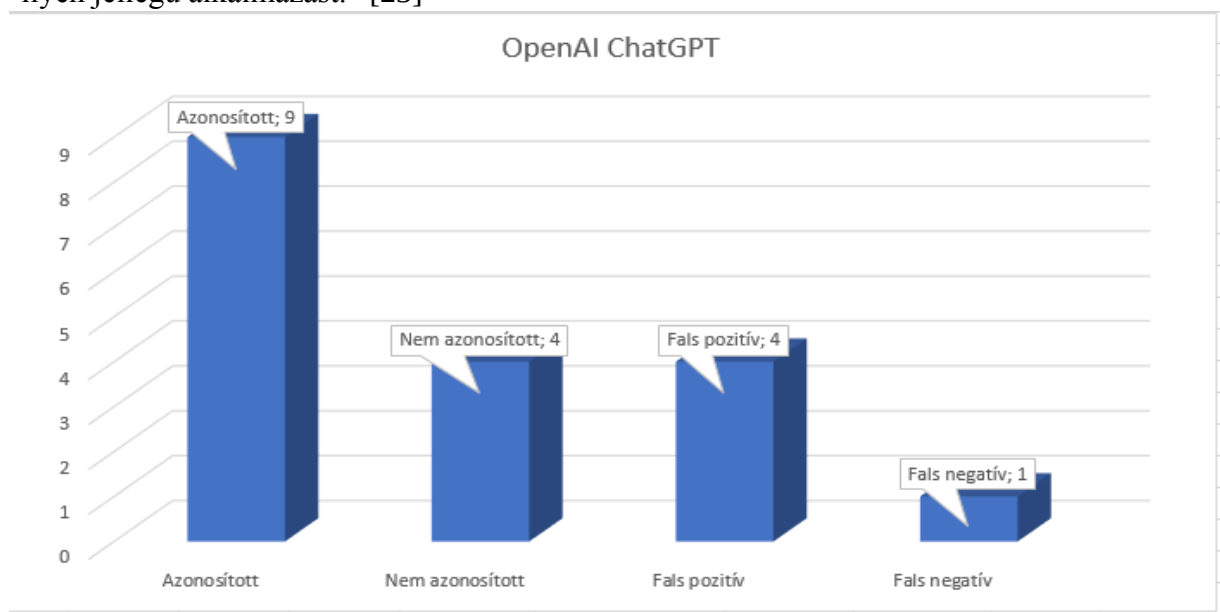
Hasonlóan a korábbi 3 modell vizsgálatához ezt a modellt is alávettem olyan mérésnek aminek során 20 támadó email kapott amiről el kellett döntenie, hogy szerinte kártékony-e.

Az adatok a grafikonon láthatóak. Amit külön kiemelnék, hogy egy támadásnál leírta, hogy nem tudja megítélni. Amit összevetve a ChatGPT-vel pozitív lépésnek tartok, mivel a ChatGPT sosem ad „nem tudom” választ, hanem mindig megmagyarázza szerinte miért van igaza. Ez értelemszerűen sok fals eredményhez vezet.” [23]



### 8.8.2. ChatGPT

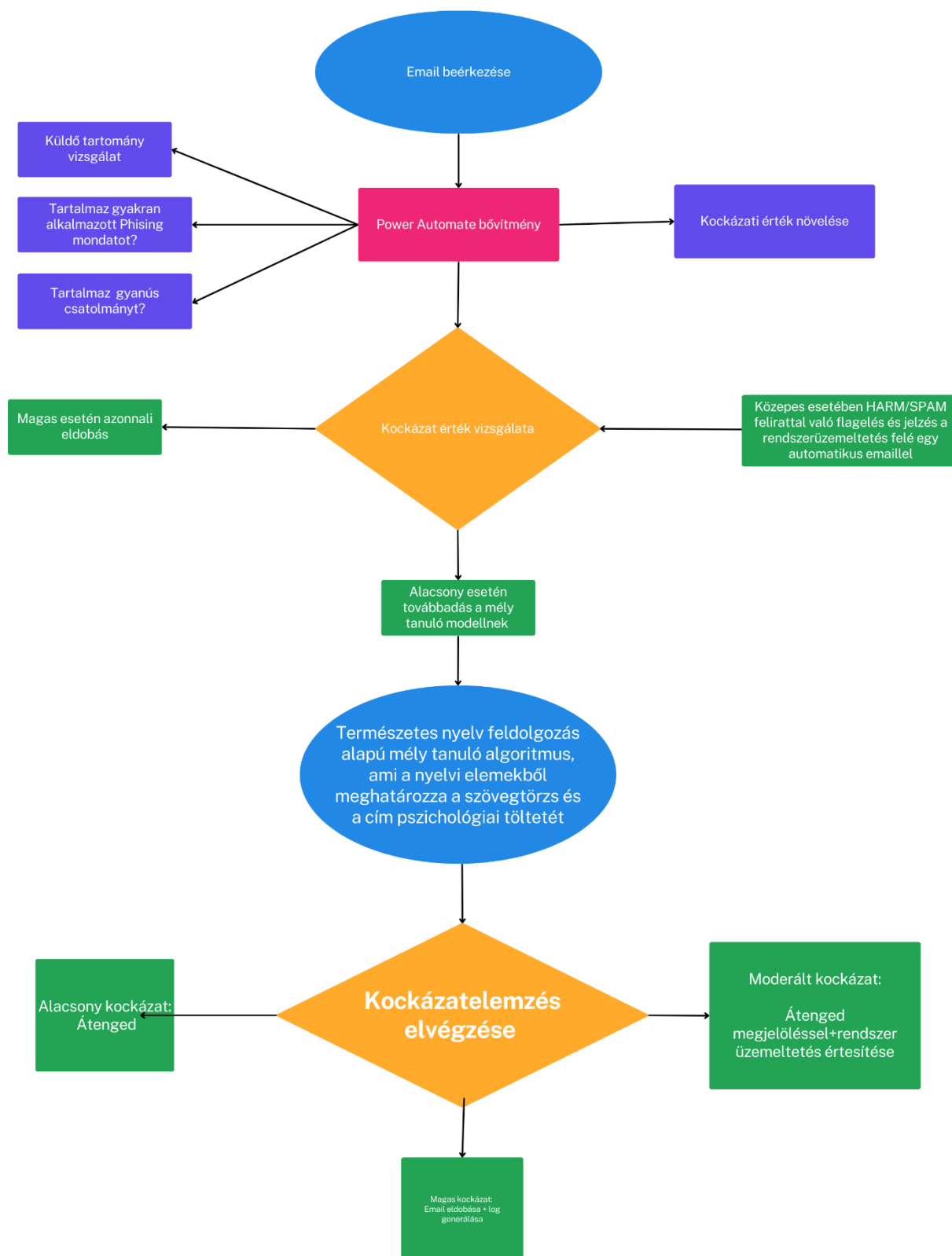
„Chat GPT-vel is elvégeztem a méréseket. Ahol elég magas azonosítási százalékot tapasztaltunk, viszont ki kell emelnem, hogy nagyon magas a fals pozitív aránya (20%). Ez valós helyzetben azt jelentené, hogy amennyiben valós email biztonságához használnánk a ChatGPT-t úgy 100 valódi emailből 20 eldobásra kerülne. Ezért jelenlegi formájában elvetem a ChatGPT ilyen jellegű alkalmazást.” [23]



## 8.9. SAJÁT MÓDSZER KIDOLGOZÁSA

Kutatásom során elkezdtem egy saját módszert kidolgozni.

Az alábbi folyamat ábrán ennek a béta verziója található. [23]



## **9. KONKLÚZIÓ - TÉZISEK**

Mivel kutatásom korai szakaszban van ezért jelenleg nem tudtam még mélyreható konklúziókat levonni.

A H1-es hipotézisemet bizonyítottam az interjúk eredményei és a saját méréseim alapján is.

A H3-as hipotézisem a szakirodalomban bizonyítást nyert, ugyanakkor a jövőben szeretném elvégezni a saját méréseimet is.

A H2, H4, H5 és H6-os hipotézisek jelenleg még nem eldönthetőek a rendelkezésre álló információkból. [23]

## 10. TÁMOGATÁS

„A KULTURÁLIS ÉS INNOVÁCIÓS MINISZTERIUM 2024-2.1.1 KÓDSZÁMÚ EGYETEMI KUTATÓI ÖSZTÖNDÍJ PROGRAMJÁNAK A NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS ALAPBÓL FINANSZÍROZOTT SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.”



## 11. IRODALJEGYZÉK

- [1] ACM CSS Téma klasszifikáció az OTDT követelmények szerint az érintett témából generálva: <https://dl.acm.org/ccs> (generálás ideje: 2023. 05. 01 22:43)
- [2] <https://terranovasecurity.com/cyber-security-statistics/> (hozzáférés: 2023. 05. 02 14:44)
- [3] Christopher Hadnagy „The Art of Human Hacking” ISBN: 978-1-118-02801-8 WileyPublishing, Inc. (2011) p.23 szerző által fordított
- [4] Kevin D. Mitnick „A legendás hacker - A megtévesztés művészete” 9789632065557
- [5] TÓTH TAMÁS „AZ EGYES SOCIAL ENGINEERING MÓDSZEREK ELHATÁROLÁSA ÉS RENDSZEREZÉSE”, Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle XVIII. évfolyam 1. szám 2020. március HU ISSN 1785-1181
- [6] Krasnyánszki Brúnó „Hogyan változtatta meg a XXI-ik századi kibervédelmet a Social Engineering?”, Évf. 4 szám 3 (2022): Biztonságtudományi Szemle Információbiztonság rovat
- [7] Dub Máté, Szakdolgozat, 'A kiberbiztonság humán aspektusának vizsgálata social engineering technikával', Nemzeti Közsolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar Közszerkezési és Infotechnológiai Tanszék Közigazgatás-szervező szak Nemzetközi közigazgatási szakirány pp, 35-50
- [8] Oroszi Eszter Diána, Biztonságtudatossági szabaduló- szoba, mint új programelem az információbiztonsági képzésekben Dunakavics A Dunaújvárosi Egyetem online folyóirata 2020. VIII. évfolyam III. szám pp 51-62
- [9] Shared Responsibility Modellről lásd a Felhő Biztonsági Szövetség megfogalmazását: <https://cloudsecurityalliance.org/blog/terms/shared-responsibility-model/> (utolsó hozzáférés 2023. 05. 03 12:24:38)
- [10] <https://www.kaggle.com/> (utolsó hozzáférés 2023. 05. 03 12:25:21)
- [11] <https://www.kaggle.com/code/mfaisalqureshi/email-spam-detection-98-accuracy> (utolsó hozzáférés 2023. 05. 03 14:13:32)
- [12] <https://www.kaggle.com/code/harshsinha1234/email-spam-classification-nlp>(utolsó hozzáférés 2023. 05. 03 14:14:43)
- [13] <https://www.kaggle.com/code/balaka18/email-spam-classification> (utolsó hozzáférés 2023. 05. 03 14:15:53)
- [14] Juan C. Lopez, Jorge E. Camargo, 'Social Engineering Detection Using Natural Language Processing and Machine Learning' 2022 5th International Conference on Information and Computer Technologies (ICICT), DOI 10.1109/ICICT55905.2022.00038
- [15] Bronjon Gogoi, Tasiruddin Ahmed, ' Phishing and Fraudulent Email Detection through
- XLIII

Transfer Learning using pretrained transformer models', 2022 IEEE 19th India Council International Conference (INDICON) | 978-1-6654-7350-7/22/\$31.00 ©2022 IEEE | DOI: 10.1109/INDI CON56171.2022.1004009

[15] S. S. S. P, S. Velpula, R. Parise, N. K. Vamsi and S. K. Chaitanya, "Phishing Attack Detection Using Convolutional Neural Networks," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 1381-1385, doi: 10.1109/ICACCS57279.2023.10113077.

[16] A. A. Abdullahi and M. Kaya, "A Deep Learning Based Method to Detect Email and SMS Spams," 2021 International Conference on Decision Aid Sciences and Application (DASA), Sakheer, Bahrain, 2021, pp. 430-435, doi: 10.1109/DASA53625.2021.9681921.

[17] A. Karthikeya, Y. B. Sai, S. Hariharan, A. C. Rao, D. Jignash and A. B. Prasad, "Prevention of Cyber Attacks Using Deep Learning," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 1332-1336, doi: 10.1109/ICACCS57279.2023.10112794.

[18] S. Tareen, S. U. Bazai, S. Ullah, R. Ullah, S. Marjan and M. I. Ghafoor, "Phishing and Intrusion Attacks: An Overview of Classification Mechanisms," 2022 3rd International Informatics and Software Engineering Conference (IISEC), Ankara, Turkey, 2022, pp. 1-5, doi: 10.1109/IISEC56263.2022.9998205.

[19] D. He et al., "An Effective Double-Layer Detection System Against Social Engineering Attacks," in IEEE Network, vol. 36, no. 6, pp. 92-98, November/December 2022, doi: 10.1109/MNET.105.2100425.

[20] Kollár Csaba A SZAKÉRTŐVÉ VÁLÁS, ILLETVE A SZAKÉRTŐK KIVÁLASZTÁSÁNAK ÉS MEGKÉRDEZÉSÉNEK MÓDSZERTANI KIHÍVÁSAI VEZETÉSTUDOMÁNY / BUDAPEST MANAGEMENT REVIEW XLIX. ÉVF. 2018. 02. SZÁM/ ISSN 0133-0179 DOI: 10.14267/VEZTUD.2018.02.07

[21] [<https://www.historyofinformation.com/detail.php?entryid=782>]

[22] [<https://www.pinecone.io/learn/series/image-search/imagenet/>]

[23] Krasnyánszki Brúnó Barnabás Óbudai Egyetem 59. Intézményi Tudományos Diákköri Konferencia Interdiszciplináris email biztonsági kihívások – kutatási jelentés

[24] <https://itbn.hu/program-2024> (utolsó hozzáférés 2024.11.02 23:42:12)

[25] [https://elearning.uni-obuda.hu/main/pluginfile.php/938646/mod\\_resource/content/1/2022-09-15%20OE%20-%20Nokia%20-%20Fundamentals%20of%20AI%20-%20Lecture%2002.pdf](https://elearning.uni-obuda.hu/main/pluginfile.php/938646/mod_resource/content/1/2022-09-15%20OE%20-%20Nokia%20-%20Fundamentals%20of%20AI%20-%20Lecture%2002.pdf)

- [26] Szilágyi Péter 2022-09-15 OE - Nokia - Fundamentals of AI - Lecture 02 p. 13
- [27] Dr. Kutor László Intelligent Systems 2023-2-2 p. 12
- [27] Phistank phistank.org elérés 2024.11.04
- [28] <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10040097>
- [29] Kollár, Csaba (2018) *A szakértővé válás, illetve a szakértők kiválasztásának és megkérdezésének módszertani kihívásai*. VEZETÉSTUDOMÁNY, 49 (2). pp. 63-75. ISSN 0133-0179
- [30] <https://www.opswat.com/products/metadefender>
- [31] Classification tree view Matlab [https://www.mathworks.com/help/examples/stats/win64/ViewingAClassificationOrRegressionTreeExample\\_01.png](https://www.mathworks.com/help/examples/stats/win64/ViewingAClassificationOrRegressionTreeExample_01.png)
- [32] Understanding Machine Learning: From Theory to Algorithms c 2014 by Shai Shalev-Shwartz and Shai Ben-David Published 2014 by Cambridge University Press.