

OTDK-dolgozat

2025

**ÓBUDAI EGYETEM
KELETI KÁROLY GAZDASÁGI KAR**



GENERATÍV AI KIBERBIZTONSÁGI KOCKÁZATAI

CYBERSECURITY RISKS OF GENERATIVE AI

Mihály Péter Richárd

Konzulens: Prof. Dr. Tick Andrea

Kézirat lezárásának dátuma: 2024. 04. 18.

TARTALOMJEGYZÉK

1.	BEVEZETÉS.....	1
2.	KUTATÁSMÓDSZERTAN	4
3.	GENERATÍV AI.....	5
3.1.	Generatív AI működésének elemzése	5
3.1.1.	AI fajták.....	6
3.1.2.	Machine Learning.....	6
3.1.3.	Deep Learning	7
3.1.4.	Artificial Neural Networks	8
3.1.5.	Natural Language Processing	9
3.1.6.	Large Language Models	9
3.1.7.	Generative Pre-trained Transformer.....	9
3.2.	GAN működése	9
3.3.	Deepfake technológiák és veszélyei.....	10
3.3.1.	Technológia	10
3.3.2.	Veszélyek	11
3.4.	Generatív modellek alkalmazása kiberbiztonsági szempontból.....	11
3.4.1.	Felhasználási területek	12
4.	KIBERTÁMADÁSOK	14
4.1.	Kiberbiztonság, kibervédelem.....	14
4.2.	Kibertámadási pontok, fenyegetések, kockázatok, támadások	15

5.	A GEN-AI ALKALMAZÁSÁNAK LEHETŐSÉGEI A KIBERTÁMADÁSOK SORÁN	17
5.1.	Kiber Ölési Lánc	18
5.2.	AI meghajtott támadások a Kiber Ölési Láncon	19
5.2.1.	Felderítési szakasz	19
5.2.2.	Hozzáférés szakasz	19
5.2.3.	Célba juttatás szakasz	19
5.2.4.	Kiaknázás szakasz	20
5.2.5.	Parancs és vezérlés (C2) szakasz.....	20
5.2.6.	Támadás végrehajtás szakasz	20
6.	GEN-AI HATÁSA A KIBERBIZTONSÁGRA DOSPERT ELEMZÉS	21
6.1.	Demográfia profil	21
6.2.	DOSPERT elemzés	21
6.2.1.	Kockázatvállalási szándék.....	22
6.2.2.	Kockázateszlelés	23
6.2.3.	Elvárt haszon	25
6.2.4.	DOSPERT értékek az alcsoportokban	27
6.2.5.	DOSPERT érték összehasonlítás a három kockázati csoportban.....	28
6.3.	Kockázat attitűd vizsgálat	29
6.3.1.	DOSPERT pontok egyénenkénti korrelációja.....	31
6.3.2.	Aspektusok közötti korreláció	32
6.3.2.1.	DOSPERT érték vizsgálata lakhely szerint.....	34

6.3.2.2.	DOSPERT érték vizsgálata foglalkozási terület szerint.....	35
6.4.	Következtetések.....	37
7.	ÖSSZEFOGLALÁS.....	38
	IRODALOMJEGYZÉK.....	39
	MELLÉKLETEK	I
	DOSPERT kérdőív kódolással	I

ÁBRAJEGYZÉK

ábra 1: Mesterséges Neurális Háló. Saját szerkesztés (Tick, 2023, p. 648) alapján	8
ábra 2: A NIST CIA hármasa. Saját szerkesztés (Chowdhury et al., 2023, p. 480) alapján	14
ábra 3: Kiberbiztonság három dimenziója. Saját szerkesztés (Mallick & Nath, 2024, p. 15) alapján	15
ábra 4: A támadók tudása és a támadások komplexitása. Saját szerkesztés (Mallick & Nath, 2024, p. 24) alapján	16
ábra 5: Cyber Kill Chain. Saját szerkesztés	18
ábra 6: Módosított Cyber Kill Chain. Saját szerkesztés	18
ábra 7: DOSPERT értékek aspektusok szerint a vizsgált alcsoportokban radar diagram	27
ábra 8: DOSPERT értékek aspektusok szerint vonal diagram	29
ábra 9: Kockázateszlelés és kockázatvállalási szándék DOSPERT pontjainak kapcsolatának buborék diagramja	32
ábra 10: Elvárt haszon és kockázatvállalási szándék DOSPERT pontjainak kapcsolatának buborék diagramja	32
ábra 11: Aspektusok közti korreláció buborék diagramja	33
ábra 12: Aspektusok közti korreláció a vizsgált csoportok szerint buborék diagram	34
ábra 13: DOSPERT pontok aspektusok szerint lakhelyenként radar diagram	35
ábra 14: DOSPERT pontok aspektusonként IT és nem IT területen dolgozók szemszögéből csoportosított oszlop diagram	36

TÁBLÁZATOK JEGYZÉKE

táblázat 1: Demográfiai profil	21
táblázat 2: Kockázat vállalási aspektusból megválaszolt kérdések eredményei	23
táblázat 3: Kockázat vállalási aspektusból megválaszolt kérdések csoportosított összesített eredményei	23
táblázat 4: Kockázateszlelés eredményei	24
táblázat 5: Kockázateszlelés csoportosított összességét eredményei	25
táblázat 6: Elvárt haszon aspektusából megválaszolt kérdések eredményei	26
táblázat 7: Elvárt haszon aspektusából megválaszolt kérdések csoportosított összesített eredményei	27
táblázat 8: DOSPERT értékek aspektusok szerint alsókálák szerint csoportosítva	28
táblázat 9: DOSPERT értékek regresszió számítás részlet	30
táblázat 10: Kockázathoz való hozzáállás kérdésenként, alcsoportok szerint.....	31
táblázat 11: DOSPERT pontok egyénenkénti korrelációja	31
táblázat 12: Aspektusok közti korreláció	33
táblázat 13: DOSPERT pontok aspektusonként ANOVA teszt eredménye.....	34
táblázat 14: DOSPERT pontok aspektusonként két mintás t-teszt eredménye	35

1. BEVEZETÉS

A mesterséges intelligencia¹ területe az elmúlt években jelentős fejlődésen ment keresztül, noha az alapok egészen az előző évszázadra nyúlnak vissza. A Church–Turing tétel alapján számítógépek bármilyen formális bizonyítást elvégezhetnek. A neurológia fejlődése során felismerték az emberi agy sok kisméretű neuronból és azok közötti kapcsolatokból álló komplexitását, amely inspirálta az elektronikus agy készítésének lehetőségét. A mesterséges intelligencia pontos definíciójának hiányában Turing egy tesztet vezetett be, amelyben a gép intelligenciával rendelkezik, ha egy megfigyelő nem tudja megkülönböztetni az emberi és gépi kommunikációt írásban. Az 1956–1974 közötti időszakot a mesterséges intelligencia aranykoraként emlegetik, de a korlátozott számítási kapacitás és a kritikák miatt következett be az "AI tél". Ezt követte egy második fellendülés, egy második tél, majd 1993–2011 közötti időszak, amikor az algoritmusok elméleti háttérét alkották meg. A 2011 óta tartó jelenlegi fejlődési szakaszt főként a Deep Learning és Big Data technikák uralják, hajtja a számítási kapacitás rohamos növekedése, valamint az internet és olcsó elektronika terjedése, amelyek lehetővé teszik a hatalmas mennyiségű adat begyűjtését és feldolgozását, ez mind elengedhetetlen a neurális hálók tanításához (Ekler & Pásztor, 2020).

A Generatív AI* (GenAI) a legújabb AI-technológiai áttörés, amely mély neurális hálózatok* segítségével képes nagy adathalmazokból tanulni és új tartalmat létrehozni. A GenAI technológia különböző típusú tartalmakat tud generálni, mint például szöveg, kép, hang, animáció, forráskód és más adatok. Az OpenAI 2022 novemberében mutatta be új, erős GenAI eszközét, a ChatGPT-t (Generative Pre-trained Transformer)*, amely megmozgatta az AI/ML* technológia egész közösségét. A ChatGPT megmutatta a GenAI technológia erejét, amellyel megváltoztathatja az emberek AI/ML-szemléletét. A technológiai iparág jelenleg versenyben áll a legkorszerűbb nagy nyelvi modellek (LLM)* létrehozásában, amelyek emberi párbeszédet tudnak folytatni, mint például a Microsoft GPT, a Google Bard és a Meta LLaMa. A GenAI az elmúlt évben elterjedt eszközzé vált az interneten. A ChatGPT két hónap

¹ Mesterséges Intelligencia (MI) = Artificial Intelligence (AI)

alatt elérte a 100 millió felhasználót a bevezetése óta, ami azt jelzi, hogy az internetezők használták a GenAI-t, vagy ismernek valakit, aki már használta (Gupta et al., 2023).²

A generatív mesterséges intelligencia (generatív AI) különleges képességeivel, mint például a Generative Adversarial Network (GAN) és deepfake technológiák, egyre inkább az érdeklődés középpontjába kerültek. Ezek működését és használatát a dolgozat 3. fejezetében mutatom be. A generatív AI képessége, hogy valósághűen szintetizáljon adatokat, olyan innovációkat hozott létre, amelyek számos területen hasznosíthatók, azonban ennek fejlődése számos kiberbiztonsági kihívást is felvet (Chowdhury et al., 2023).

Jelen dolgozat a generatív AI kiberbiztonsági aspektusait vizsgálja meg, célja a technológia kockázatainak és veszélyeinek mélyebb megértése, valamint hatékony védekezési és szabályozási stratégiák kifejlesztése. A dolgozat kitér a generatív AI által alkalmazott technológiák alapelveire, körüljárja a deepfake technológiák és GAN működését, és bemutatja, hogy ezek a fejlett modellek milyen kiberbiztonsági problémákat hozhatnak magukkal.

A felvetett probléma középpontjában az áll, hogy miként használhatják a kiberbűnözők és más potenciális támadók a generatív AI-t különféle kibertámadásokban, beleértve az adatvesztést, szivárgást és az álhírek terjesztését. Emellett a dolgozat olyan veszélyekre is kitér, amelyek a generatív AI alkalmazásából eredhetnek, például a manipuláció és az információ torzítása, amelyek súlyos következményekkel járhatnak a társadalmi és gazdasági szinteken.

Az elemzés során kiemelt hangsúlyt fektetek a kibertámadások feltárására, a generatív AI kiberbiztonsági kockázataira. A kockázatokat kvantitatív kutatás keretein belül is vizsgálom.

Fontos megjegyezni, hogy a dolgozat egyesével részletesen nem kíván foglalkozni a generatív AI tartalomgyártó alkalmazásaival, például a művészeti területeken vagy kreatív iparágakban történő felhasználással. Az elemzések során hangsúlyozom azokat a területeket, ahol a generatív AI kockázatokat hordoz, és amelyek kiemelt figyelmet igényelnek a kiberbiztonság terén.

A továbbiakban részletezésre kerülnek a generatív AI működésének alapelvei, a kibertámadások módjai, potenciális pontjai, illetve a generatív AI felhasználási módjai mind

² A csillaggal (*) jelölt fogalmak kifejtésére a 3. fejezetben kerül sor.

kibervédelmi és kibertámadási oldalról. A védekezési stratégiák kidolgozása, valamint az etikai és jogi kihívások elemzése már nem a dolgozat része. A dolgozat zárásaként összefoglalom a kutatás eredményeit, és felvázolom a jövőbeli kilátásokat a generatív AI kiberbiztonsági területén.

2. KUTATÁSMÓDSZERTAN

A jelen kutatás során a generatív mesterséges intelligencia (generatív AI) kiberbiztonsági kockázataival kapcsolatos elméleti háttérrel, szakirodalmi kutatást és elemzést szekunder kutatási módszerrel végeztem. Az elméleti keretrendszer kialakítása érdekében igyekeztem körültekintően keresni a generatív AI kiberbiztonsági kockázatait érintő releváns szakirodalmakat a ResearchGate, Scopus és IEEE Xplore, Google Scholar online adatbázisaiban.

A kutatás során alkalmazott kulcsszavak a következők voltak: „artificial intelligence”, „generative artificial intelligence”, „generative adversarial network”, „cybersecurity”, „AI security”, „adversarial attacks”, „cyber security”, „cyber security risks”, „cyber security with ai”, „cyber security with artificial intelligence”, „ai risks”, „artificial intelligence in cyber security”, „risks of artificial intelligence in cyber security”, „attack with ai”. A kutatási témámra vonatkozó címek, kulcsszavak és absztraktok alapján választottam ki a releváns szakirodalmi forrásokat a kutatási kérdéseim megválaszolásához.

A primer kutatásban kvantitatív kutatási módszert alkalmaztam, amelyhez kérdőívet használtam az adatok gyűjtésére. A DOSPERT (Domain-Specific Risk-Taking) skála segítségével készítettem el a kérdőívet. Ez a pszichológiai mérőeszköz a személyes kockázatvállalási hajlandóságot méri különböző területeken, például pénzügyek, egészség és biztonság. A kutatás során megvizsgáltam a résztvevők hajlandóságát a generatív AI kiberbiztonsági kockázataival kapcsolatos személyes magatartás és döntéshozatal tekintetében (Blais & Weber, 2006).

Az adatok feldolgozását a MS Excel és az SPSS v25 szoftverek segítségével végeztem el, hogy részletes statisztikai elemzéseket készítek a kapott válaszok alapján. A kvantitatív kutatás célja az összefüggések, tendenciák és szignifikáns tényezők azonosítása a generatív AI kiberbiztonsági kockázatai és a résztvevők válaszai között. A kvantitatív kutatás DOSPERT skála segítségével készített kérdőív eredményeinek értékelésével történt, ahol megnéztem a kockázatvállalási szándékot, a kockázat észlelés fokát és az elvárt haszon értékeit.

3. GENERATÍV AI

3.1. Generatív AI működésének elemzése

A generatív modellek története egészen a 1950-es évekig nyúlik vissza, amikor kifejlesztették a Rejtett Markov Modelleket (Hidden Markov Models (HMMs)) és a Gauss-keverék Modelleket (Gaussian Mixture Models (GMMs)). A mély tanulás megjelenésével ezen generatív modellek teljesítményében jelentős ugrás következett be. Az egyik korai szekvencia-generálási módszer az N-gram nyelvmodellezés volt, ahol a legjobb sorozat a megtanult szóeloszlás alapján generálódott. A Generatív Ellentmondásos Hálózat (Generative Adversarial Network (GAN)) bevezetése jelentősen fokozta ezeknek a modelleknek a generatív erejét. A legújabb technológia, amely a generatív technológia gerincét képezi, a transformer architektúra, amelyet alkalmaztak olyan nagy nyelvi modelleken, mint a BERT és a GPT. A GenAI számos területen fejlődött, mint például a kép-, beszéd-, szöveg alkotás (Gupta et al., 2023).

A Generatív AI működésének megértéséhez szükséges pár alapvető fogalmat tisztáznunk. Elsősorban meg kell ismernünk magának az AI-nak (Artificial Intelligence) az alapvetéseit. A következőkben vázlatosan bemutatom az alapvető pilléreket.

Tudományos cikkekben sokféle meghatározás található, de talán a legkönnyebben érthetők a következők:

- Mesterséges intelligencia (MI) egy módszer arra, hogy a gépek intelligensen gondolkodjanak és viselkedjenek (fordítás:(Joshi, 2017, p. 8)).
- A mesterséges intelligencia olyan számítógépes rendszerek leírására használható, amelyek emberi intelligenciát és kognitív képességeket mutatnak, például a következtetés, mintázatfelismerés és bonyolult adatok értelmezése terén (fordítás: (Jaggia et al., 2023, p. 386)).
- A mesterséges intelligencia (MI) az a képesség, amely lehetővé teszi egy számítógépes rendszer számára, hogy olyan feladatokat végezzen, amelyek általában emberi intelligenciát igényelnek (fordítás: (Kinicki & Soignet, 2022, p. 287)).

3.1.1. AI fajták

Az AI-kat három különálló csoportra lehet bontani.

1. **Artificial Narrow Intelligence (ANI)** - Mesterséges Keskeny Intelligencia, ismertebb nevén „weak AI”, tehát gyenge Mesterséges Intelligencia, limitált funkcionalitással rendelkezik, limitált feladatok ellátására. Például e-mail spamszűrők, filmajánló rendszerek vagy online vásárlási webhely ajánló rendszerek (Kalota, 2024).
2. **Artificial General Intelligence (AGI)** - Mesterséges Általános Intelligencia, másnéven „strong AI”, vagyis erős Mesterséges Intelligencia, az ANI következő szintje. Az ilyen AGI-k feladata, hogy olyan kapacitási szinten végezzenek el feladatokat, mint az emberek. Az AGI-k lényegében arra valók, hogy olyan gépeket hozzanak létre, amik folyamatosan tanulnak és fejlesztik magukat és megkülönböztethetetlenek az emberektől (Kalota, 2024).
3. **Artificial Super Intelligence (ASI)** - Mesterséges Szuper Intelligencia, ezen AI már különbözik az Általános Mesterséges Intelligenciától, ez az AI még csak elméleti, szakértők úgy határozzák meg, hogy "minden tekintetben lényegesen intelligensebb az embernél". Ezeknek a gépeknek saját szükségleteik, hitük és vágyaik lehetnek (Kalota, 2024).

A mai világban legelterjedtebb AI koncepció az ANI vagyis a gyenge AI, ennek is különböző fajtái vannak, annak függvényében, hogy mire akarják használni őket, vagy milyen speciális területen akarják használni őket (Kalota, 2024). Az AGI teljes megvalósítása még évekre van, de már használják őket az egészségügyben, oktatásban, gyártásban főleg DeepLearning és neurális hálók technológiáival kiegészítve (Gordon, 2023)

3.1.2. Machine Learning

Ahhoz, hogy a gépek intelligensen tudjanak viselkedni, tanulniuk kell, mint az embernek is. A gépi tanulás (Machine Learning) az AI egy része, részhalmaza. Több definícióból talán a legegyszerűbben érthető: A gépi tanulás „lehetővé teszi, hogy a számítógép automatikusan, emberi beavatkozás vagy segítség nélkül tanuljon”(Kalota, 2024, p. 3). Lényegében a gépi tanulás nem más, mint algoritmusok és technikák összessége, amik segítségével a gépek tanulni tudnak adatokból (Kalota, 2024)

A gépi tanulásnak két kategóriája létezik:

1. **Supervised Machine Learning (SML)** - Ellenőrzött Gépi Tanulás, ezen folyamatnál van egy felügyelő (vagy ha úgy tetszik tanár), akinek az a feladata, hogy címkézett adatokkal tanítsa a gépet. Például egy ilyen tanítási folyamatnál a tanár mutat sok-sok képet almákról, amik minden egyes alkalommal meg vannak címkézve, hogy ezek almák. A következő lépésben a tanár elővesz egy másik adathalmazt, egy másik képgyűjteményt, amiket megmutatva, a gépnek az a feladata, hogy pontosan megállapítsa, hogy van-e, a már megtanult minták alapján alma a képeken (Kalota, 2024).
2. **Unsupervised Machine Learning (USML)** - Nem Ellenőrzött Gépi Tanulás, ahogy a neve is állítja, tanár nélkül történik, a gépnek az a feladata, hogy saját maga analizálja az adatokat és találjon mintákat, és ezen minták alapján alkosson különböző kategóriákat. Például, egy ilyen gépnek odaadunk több ezer képet almákról, banánokról és narancsokról. Ezen adathalmazon a gépnek mintákat kell keresen, mint alak, textúra, szín. Majd ezeket a mintákat külön kategorizálva, ezen minták alapján azonosítja sorjában a fent említett gyümölcsöket (Kalota, 2024).

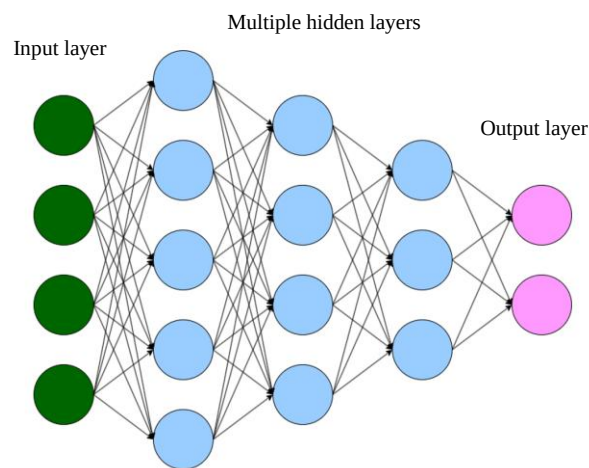
3.1.3. *Deep Learning*

A mély tanulás (Deep Learning) fő különbsége a gépi tanulástól, hogy míg a gépi tanulás főként strukturált adatokkal dolgozik, vagy strukturálatlan de előzetesen feldolgozott adatokkal dolgozik, a mély tanulás strukturálatlan adatokat használ és az adatok nincsenek előzetesen feldolgozva (Kalota, 2024).

További különbségek: a gépi tanulás esetén viszonylag kis mennyiségű adat elegendő a tanításhoz, és az alacsonyabb kategóriás CPU-k is képesek a feladatokra. Emellett a modell betanítása viszonylag gyorsan elvégezhető. Ezzel szemben a mély tanulás nagy adatmennyiséget igényel a hatékony tanításhoz, és csúcskategóriás számítási teljesítményre, illetve grafikus feldolgozó egységre (GPU), van szükség (Kalota, 2024, tbl. 1). A mély tanulást az emberi agy inspirálta és Mesterséges Neurális Hálókat (Artificial Neural Networks (ANN)) használ. Ahhoz, hogy megértsük a mély tanulást, kis betekintést kell nyernünk a Mesterséges Neurális Hálózatok világába (Kalota, 2024).

3.1.4. Artificial Neural Networks

A tanulás, a memória és az általánosítás beépítése reprodukálja az agy idegrendszeri felépítését. Következésképpen a neurális hálózatok képesek megragadni az adatokon belüli bonyolult kapcsolatokat, és alapelemként szolgálhatnak a fejlett gépi tanulási rendszerekben, amelyeket általában mély tanulásnak neveznek (fordítás: (Jaggia et al., 2023, p. 435)). Az 1. ábra szemlélteti, hogy egy ilyen ANN több rétegből áll, az első az úgynevezett bemeneti réteg (vagy „input layer”), ezután következik több rejtett réteg, ahol rétegenként számítások végződnek és a kimenetet továbbadják egy következő rejtett rétegnek. Egyik rejtett réteg bemenetként használja egy korábbi réteg kimenetét, mindaddig amíg a kimenet el nem ér az „Output Layer”-hez (vagyis a kimeneti réteghez), ami biztosítja a végleges eredményt vagy előrejelzést (Kalota, 2024).



ábra 1: Mesterséges Neurális Háló. Saját szerkesztés (Tick, 2023, p. 648) alapján

Most, hogy megismertük, mennyire is összetett egy ilyen rendszer, alap tudást szereztünk a Mesterséges Intelligenciáról, a Gépi Tanulásról, Mély Tanulásról és az ehhez tartozó Mesterséges Neurális Hálózatokról, elérkeztünk a Generatív AI-hoz, röviden Gen-AI. Az, hogy „generatív” azt jelenti, hogy ez a típusú AI képes „generálni”, létrehozni, alkotni. Ez a fogalom olyan algoritmusokat foglal magába (pl.: ChatGPT), amik képesek új tartalmat előállítani, mind hang, kód, képek, szöveg, szimulációk és videók területén (Kalota, 2024).

Ahhoz, hogy jobban megértsük mi is az a Gen-AI, mi is az a ChatGPT, meg kell ismernünk a Természetes Nyelvi Feldolgozás (Natural Language Processing (NLP)), Nagy Nyelvi Modellek (Large Language Models (LLM)) és a Generatív Előképzett Transzformer (Generative Pre-trained Transformer (GPT)) koncepcióit (Kalota, 2024).

3.1.5. Natural Language Processing

Az emberi nyelv analizálásához, tanulásához és generálásához tervez és használ számítógépes programokat, azért, hogy idővel a számítógép értelmezni tudja, hogy mit mond neki a felhasználó (Kalota, 2024).

3.1.6. Large Language Models

A nyelvi modell (LM) lehetővé teszi számunkra, hogy „megjósoljuk, milyen szavak következnek egy szövegben, és ezáltal javaslatot tegyünk egy e-mail vagy szöveges üzenet befejezésére” (Russell et al., 2021, p. 824).

3.1.7. Generative Pre-trained Transformer

A transzformerek egyfajta Mesterséges Neurális Hálózatok, inputokat alakítanak át egyik formátumból a másikba, például szöveges inputra képet vagy hangot ad vissza outputként. A GPT modellek, az ANN modellek egy családja, amik az inputként kapott, úgynevezett „prompt”-ok alapján szavak, kódok vagy egyéb adatalapú sorozatokat állítanak elő. A legismertebb ilyen GPT a ChatGPT, ami ANN, NLP és LLM modellek kombinációját használja (Kalota, 2024).

A ChatGPT berobbanása után váltak egyre népszerűbbé a különböző generatív AI-k, amik más és más célt szolgálnak. Ilyenek például a Bing Image Creator, a DALL-E2, a DreamStudio by Stability AI. Az ilyen modellek kép-generátor nyelvi modellek szöveges és képes adatokkal vannak tanítva, így ezek képeket tudnak előállítani szöveges „prompt” üzenetekből (Kalota, 2024).

3.2. GAN működése

A GAN, a Generative Adversarial Networks betűszava, ami lefordítva a Generatív Versengő Hálózatokat jelenti. Ez a típusú technológia segíti a számítógépeket komplex mintázatok megtanulásában, anélkül, hogy nagy mennyiségű címkézett tanító adatra lenne szükség. A GAN-ok két hálózatot egymással versenyeztetve működnek. Az egyik hálózat létrehozza az adatot, a másik különbséget próbál tenni a valós és a generált adat között. Ezen a versenyhelyezeten keresztül fejlődnek és tanulnak a hálózatok, hogy realisztikus adatokat hozzanak létre (Creswell et al., 2018). Az ilyen megtanult reprezentációknak különféle hasznos

felhasználási területei vannak. Új képek létrehozására, képek jelentős szerkesztésére használhatók, vagy akár a képek stílusát lehet velük megváltoztatni, és javítani a kép minőségét (Creswell et al., 2018).

A GAN-ok a számítógépek tanításának egy új, leleményes módja, főleg akkor, ha nincs sok példánk a tanításhoz. 2014-ben mutatták be őket és lényegében olyan, mint egy versengő páros – az egyik a művész (generátor), aki hamis képeket készít, a másik a szakértő (diszkriminátor), akinek az a dolga, hogy kiszúrja és elkülönítse a hamis képet az igaziaktól (Creswell et al., 2018). A művész (generátor) nem fér hozzá az eredeti képekhez, csak a szakértő visszajelzéseire alapoz. A szakértő (diszkriminátor) viszont hozzá fér mind a hamisítványokhoz, mind az igazi képekhez. A szakértő dolga, hogy rájöjjön melyik-melyik, és visszajelzést adjon róla. Mindketten tanulnak és az egymással való versengés által lesznek egyre jobbak (Creswell et al., 2018).

Egy ilyen GAN ezer meg ezer fotót dolgozhat fel egy személyről, majd próbál egy új portrét készíteni, anélkül, hogy a kép tökéletes másolata lenne bármelyik korábbiak. Kutatások szerint, a GAN-ok még kevesebb információval tanítva lesznek képesek képeken, videókon szereplő személyek fejét, teljes testét, vagy akár hangjukat elcserélni (Westerlund, 2019).

3.3. Deepfake technológiák és veszélyei

3.3.1. Technológia

A deepfake elnevezés a „deep learning”, tehát mély tanulás és a „fake”, tehát hamisítvány szavak kombinációjából ered. Olyan realiztikus, digitálisan manipulált videók létrehozására használják, ami a hallgatóság megtévesztése érdekében jött létre, például a videón szereplő olyat csinál és/vagy mond, ami valójában nem történt meg (Westerlund, 2019). A deepfake-ek neurális hálózatokra támaszkodnak, amik nagy mennyiségű adat mintákat analizálva tanulják meg egy személy arckifejezéseit, modorát, hangját és ragozását utánozni. A tanulási folyamat során két személyről készült videós anyagot adnak a mély tanuló algoritmusnak arra képezve, hogy megcserélje ennek a két személynek az arcát. Ehhez arc feltérképező technológiát és Mesterséges Intelligenciát használnak (Westerlund, 2019). A deepfake-ek 2017-ben láttak napvilágot, amikor egy Reddit felhasználó kompromitáló videókat töltött fel közszereplőkről, híres személyekről. A deepfake-eket nehéz érzékelni, mert valódi felvételeket használnak,

valóságosnak tűnő hangzással, és arra vannak optimalizálva, hogy a közösségi platformokon gyorsan terjedjenek (Westerlund, 2019).

Az alacsony minőségű, alig megszerkesztett olcsó hamisítványok (Cheap fakes) előállításához szükséges alacsony árú hardverek (pl. hatékony grafikus feldolgozó egységek) széleskörben elérhetők, így az ilyen hamisítványok már mindenhol jelen vannak. A kiváló minőségű, realisztikus dezinformáló deepfake-ek előállítására szolgáló szoftverek egyre inkább nyílt forráskódúként érhetők el. Ezen eszközök felhasználásával, kevés technikai tudással, művészeti szakértelemmel nem rendelkező felhasználók is közel tökéletesre tudnak szerkeszteni videókat, kicserélni arcokat, módosítani kifejezéseket és beszédet szintetizálni (Westerlund, 2019). Technológiai szempontból, a deepfake-ek a korábban bemutatott GAN-ok termékei. Két Mesterséges Neurális Hálózat dolgozik együtt, hogy valósághű médiát hozzanak létre (Westerlund, 2019).

3.3.2. Veszélyek

A vállalati világ már kifejezte érdeklődését a vírusos csalások elleni védelem iránt, mivel a deepfake-eket piaci és tőzsdei manipulációra is fel lehet használni, például úgy, hogy egy vezérigazgató rasszista vagy nőgyűlölő gyalázkodásokat mond, hamis egyesülést jelent be, hamis nyilatkozatokat tesz pénzügyi veszteségekről vagy csődről, vagy a deepfake segítségével úgy állítják be őket, mintha bűncselekményt követnének el. Továbbá a deepfake technológia lehetővé teszi egy vezető valós idejű digitális megszemélyesítését, például arra, hogy megkérjen egy alkalmazottat sürgős készpénzáttutalás végrehajtására vagy bizalmas információk megadására (Westerlund, 2019).

Ezenkívül a deepfake technológia csalárd személyazonosságot hozhat létre, és az élő közvetítésű videókban egy felnőtt arcát gyermek vagy fiatalabb személy arcává alakíthatja, ami aggályokat vet fel a technológia gyermekragadozók általi használatával kapcsolatban (Westerlund, 2019).

3.4. Generatív modellek alkalmazása kiberbiztonsági szempontból

Az AI nem csak veszélyeket és kockázati faktorokat hordoz magával, probléma megoldóként is tud funkcionálni. A kognitív adatfeldolgozás és az AI kibertámadások felfedezésére, ellenük való védekezésre és a támadások vizsgálatára is használva vannak (Vähäkainu & Lehto, 2019).

A kiberbiztonsági intézkedések a kockázatok kezeléséhez, a sebezhetőségek javításához és a rendszer ellenálló képességének javításához kapcsolódnak. A modern információbiztonsági megoldások vagy ember által, vagy gép által készültek. Az úgynevezett analitikai megoldások IT biztonsági szakértők szabályain alapulnak, amelyek figyelmen kívül hagyják azokat a támadásokat, amelyek nem felelnek meg a megállapított szabályoknak. A gépi tanulás alapú megközelítés az olyan anomáliák azonosítására támaszkodik, amelyek azonosíthatják a hamis pozitív eredményeket, bizalmatlanságot keltve a rendszerrel szemben, és így emberi erőfeszítést igényelnek az esetek kivizsgálásához (Vähäkainu & Lehto, 2019).

3.4.1. Felhasználási területek

Biztonsági műveletek és incidensekre való reagálás

1. AI2: AI amely a kibertámadások előrejelzésére szolgál (Vähäkainu & Lehto, 2019).
2. CylanceProtect: Egy integrált információbiztonsági fenyegetésmegelőző eszköz, amely egyesíti a mesterséges intelligencia előnyeit az információbiztonsági ellenőrzésekkel a rosszindulatú programok fertőzéseinek megelőzése érdekében (Vähäkainu & Lehto, 2019).
3. DarkTrace: Egy információbiztonsági megoldás, amely segíthet felismerni és azonosítani a felmerülő számítógépes fenyegetéseket, amelyek képesek megkerülni a hagyományos információbiztonsági védelmet (Vähäkainu & Lehto, 2019).

Webes biztonság

1. Cyberlytic profiler: Egy olyan eszköz, amely a webhelyekre irányuló veszélyeket azonosítja. Mesterséges intelligenciával működik, hogy felismerje és rangsorolja a kibertámadásokat az adatokra jelentett kockázat alapján (Vähäkainu & Lehto, 2019).
2. Amazon Macie: Egy gépi tanulást alkalmazó információbiztonsági szolgáltatás. Segítségével az érzékeny adatokat azonosítják, osztályozzák és védelmezik (Vähäkainu & Lehto, 2019).

Végpont biztonság

1. Deep Instinct: Valós időben nyújt védelmet a szervezet mobileszközeinek és szolgáltatásainak az ismert és ismeretlen támadásokkal szemben. Képes észlelni, azonosítani és megakadályozni a rosszindulatú szoftverek tevékenységét a szervezet minden szintjén. (Vähäkainu & Lehto, 2019).

2. SparkCognition DeepArmor: Felismeri és megakadályozza a rosszindulatú programok, vírusok, férgek, trójaiak és ransomware programok által jelentett fenyegetéseket (Vähäkainu & Lehto, 2019).
3. Vectra Networks Cognito: mesterséges intelligenciát alkalmaz, hogy részletes és valós idejű képet készítsen az aktuális kibertámadásokról, és reagáljon rájuk (Vähäkainu & Lehto, 2019).

Mobil biztonság: Az IBM MaaS360 az IBM által kifejlesztett mobil eszközközkezelő alkalmazás, amely biztosítja a szervezet összes személyes mobil eszközét, alkalmazását, tartalomkezelését és kiberbiztonságát. A rendszer elkülöníti a potenciális szervezeti üzleti titkokat a mobileszközre telepített alkalmazásoktól, illetve a szervezetek korlátozhatják az alkalmazottak adathozzáférési jogait is, és a magasabb hozzáférési jogokat meghatározott feladatokhoz csak nagyon ellenőrzött módon engedélyezhetik (Vähäkainu & Lehto, 2019).

Fenyegetés felderítés: Az IBM QRadar Advisor with Watson az IBM Watson mesterséges intelligenciáját alkalmazza a QRadar Security Platform információbiztonsági elemzésre tervezett platformon belül. Fő feladata a rejtett fenyegetések felfedése és a fenyegetések hitelesítési folyamatának automatizálása. A QRadar és a Watson legfontosabb jellemzői az automatizált fenyegetésvizsgálatok, a mesterséges intelligencia használata és a magas szintű kockázatok észlelése (Vähäkainu & Lehto, 2019).

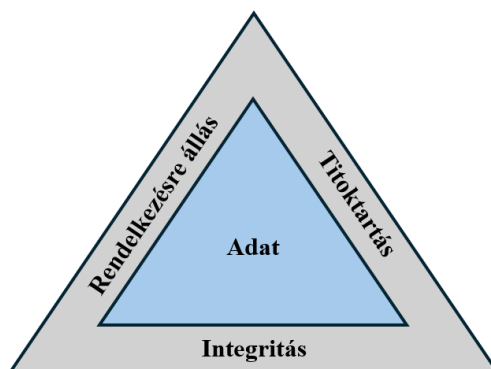
Emberi biztonság: Az IBM QRadar UBA (User Behavior Analytics) alkalmazásba beépített gépi tanulási algoritmusok segítenek a szokásos felhasználói viselkedés megértésében és az ezektől való releváns eltérések felismerésében. Ezek a gépi tanulási algoritmusok specifikusan a gyanús és rendellenes végfelhasználói viselkedés észlelésére lettek tervezve. Az algoritmusok képesek azonosítani és jelenteni a rendellenes viselkedést, és elindítják az UBA alkalmazást, amelynek felhasználói kockázati pontszámai igény szerint növekednek (Vähäkainu & Lehto, 2019).

4. KIBERTÁMADÁSOK

Annak érdekében, hogy betekintést nyerjünk a GenAI kibertámadásokban való felhasználási lehetőségeibe, úgy gondoltam, hogy először kitérek a kiberbiztonságra, a kibertámadásokra, listázom a leggyakoribb fenyegetéseket, támadási típusokat. Ebben a fejezetben szakmai irodalomra támaszkodva először a kiberbiztonsági fogalmakról, elvekről, modellekről írok, majd a kiberfenyegetéseket és kiberbiztonsági kockázatokat, illetve a kibertámadásokat mutatom be. Kutatómunkám során a „cyber security”, „cyber security risks”, „cyber security with ai”, „cyber security with artificial intelligence”, „ai risks”, „artificial intelligence in cyber security”, „risks of artificial intelligence in cyber security”, „attack with ai” keresőszavakat használtam.

4.1. Kiberbiztonság, kibervédelem

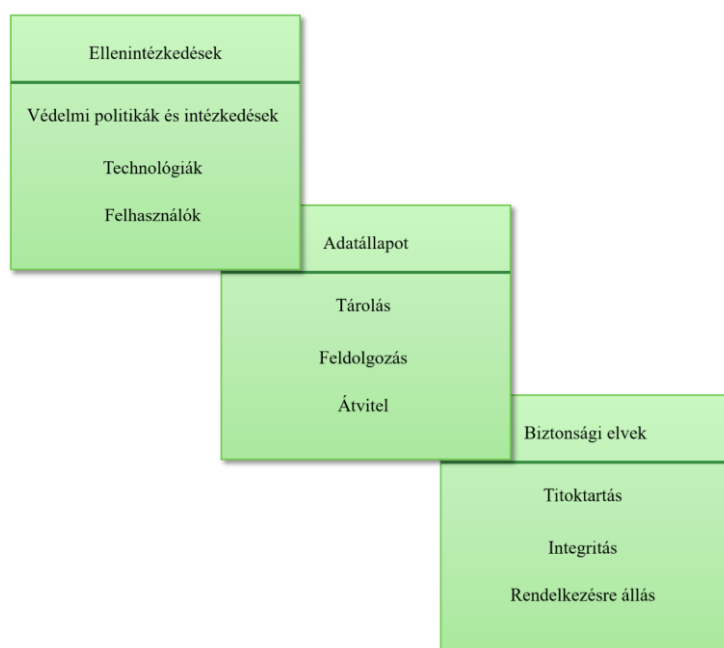
Kutatásom során a Researchgate adatbázisában találtam rá (Refsdal et al., 2015) könyvében a kiberfenyegetés és kiberbiztonság fogalmára, mely szerint egy kiber-fenyegetés, olyan fenyegetés, ami kihasználja a kiberteret (2015, p. 29) és, hogy a kiberbiztonság a kiber-rendszerek nyújtotta védelem a kiber-fenyegetésekkel szemben (2015, p. 29). Az NIST (National Institute of Standards and Technology) meghatározott egy úgy nevezett „CIA hármast”, ami 3 információbiztonsági/kiberbiztonsági elvből áll (2. ábra). Kiberbiztonsági rendszerek létrehozásánál/üzemeltetésénél biztosítanunk kell ezen hármast állandó meglétét.



ábra 2: A NIST CIA hármasa. Saját szerkesztés (Chowdhury et al., 2023, p. 480) alapján

Confidentiality (titoktartás), C, mely elv szerint az adatokhoz vagy információkhoz engedély nélkül senki nem férhet hozzá. **Integrity (integritás), I** és kiterjesztései: hitelesítés és letagadhatatlanság, mely elv szerint a tárolt vagy átvitel alatt álló adatokat vagy információkat nem lehet módosítani vagy megsemmisíteni. Kiterjesztése a letagadhatatlanság (ha mi vagy a szoftverünk a nevünkben tranzakciót követett el, azt később nem tagadhatjuk le) és hitelesség

(mi vagy szoftverünk jogosult a működésre). Valamint **availability (rendelkezésre állás)**, A, mely elv szerint minden olyan esetben, amikor az információ vagy adat jogosult felhasználója hozzá kíván férni, annak rendelkezésre kell állnia. Az általunk fejlesztett, akár AI alapú szoftver működése során bármelyik elv megsértésének jogi következményei lehetnek (Chowdhury et al., 2023). Ezen kibervédelmi elvekre épül egy háromdimenziós kiberbiztonsági modell (3. ábra).

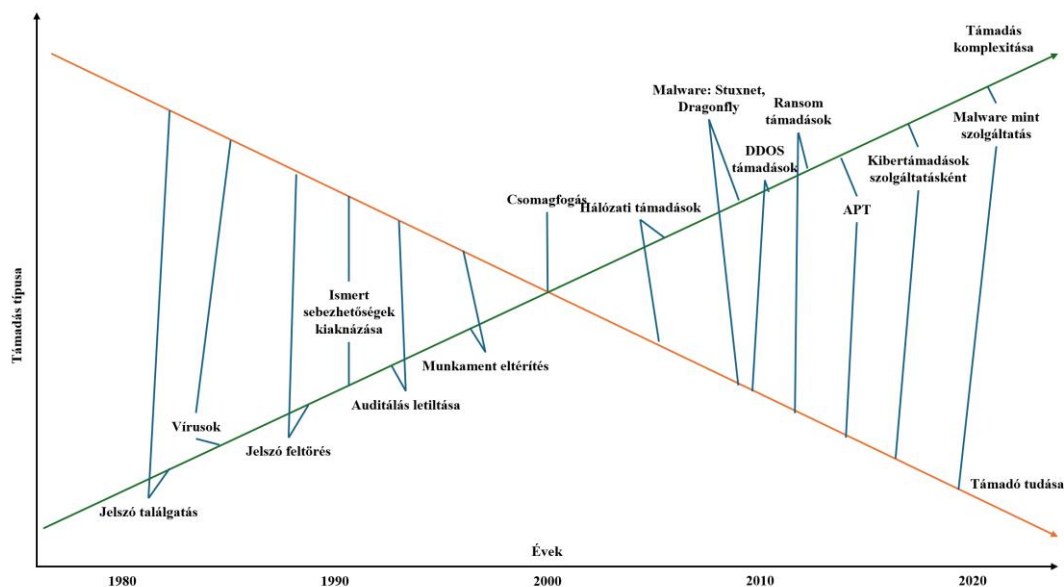


ábra 3: Kiberbiztonság három dimenziója. Saját szerkesztés (Mallick & Nath, 2024, p. 15) alapján

Ez a háromdimenziós modell különböző aspektusait öleli fel a kibervédelemnek. Az alapja, a korábban tárgyalt CIA elvek, ezen támaszkodik a második dimenzió, ami az adatok biztonságáért felel. Itt fontos megjegyeznünk, hogy ez a dimenzió az adat minden alakjában felelős a védelemért, tehát lefedi az adatok tárolását, feldolgozását és átvitelét. A harmadik és egyben legfelső dimenzió az ellenintézkedések rétege, ami magában foglalja a politikák és gyakorlatok megfogalmazását és végrehajtását, az új technológiák integrálását és a felhasználói tudatosság növelését (Mallick & Nath, 2024).

4.2. Kibertámadási pontok, fenyegetések, kockázatok, támadások

A kibervédelem fejlődésével egyenes arányosan nőtt a kibertámadások száma, típusa és az általuk okozott kár (Mallick & Nath, 2024). Mégis, a kibertámadások komplexitása és a támadók technikai tudása között fordított arányosságot tapasztalhatunk (4. ábra).



ábra 4: A támadók tudása és a támadások komplexitása. Saját szerkesztés (Mallick & Nath, 2024, p. 24) alapján

A dolgozatban nem térek ki az alapvető kiberbiztonsági fenyegetések típusainak részletes tárgyalására (számítógépes vírus, féreg, trójai faló, rootkit, hackertámadások, kémprogram, rémíró program, Vics program, zsarolóvírusok, távoli hozzáférés, szoftveres sebezhetőség, biztonsági rések, vezeték nélküli hálózatok vagy operációs rendszerek, webszolgáltatók sebezhetősége, szippantó támadások, hamisító támadások) azok kockázataira és sebezhetőségére, a vizsgálatot leszűkítettem a generatív AI területére, és az ott lehetséges támadási megoldásokra.

A kibertámadások lehetséges fajtái:

Szociális manipulációs támadások, Alkalmazástámadások, Kriptográfiai támadások, Eltérítési támadások, Számítógépes hálózati támadások (Computer Network Attacks (CNA)), Adathalász támadások, Malware támadások, Botok és botnetek, Jelszavas támadások, Közbeékelődési támadás (Man-in-the-middle attack) (Mallick & Nath, 2024).

5. A GEN-AI ALKALMAZÁSÁNAK LEHETŐSÉGEI A KIBERTÁMADÁSOK SORÁN

Ebben az alfejezetben mutatom be a generatív AI alkalmazásának lehetőségeit kibertámadásokban, amiket a kutatott publikációkból gyűjtöttem össze. Ebben a fejezetben az angol nyelvű források részeit, általam készített fordításban találhatók némi egyszerűsítéssel, a könnyebb érthetőség céljából.

A kibertámadások területét a kibertámadási eszközök és legújabb technikák folyamatos fejlődése alakítja és tágítja. Ennek eredményeként a kiberteret megnyitják a különböző, hatékony és negatív hatású kiberfegyverek előtt. Az AI rosszindulatú felhasználása lehetővé teszi, hogy a számítógépes fenyegetéseket automatizáltan és nagy mértékben skálázzák. A mesterséges intelligencia segítségével a kiberbűnözők könnyen alkalmazkodhatnak a védekező intézkedésekhez, rendkívül gyorsan hajthatnak végre támadásokat, és pontosan kihasználhatják a sebezhetőségeket. Az AI lehetőséget ad a támadóknak arra, hogy utánozzák az emberi viselkedést, ami azt eredményezi, hogy az adathalász támadások meggyőzőbbek és nagyobb valószínűséggel vezetnek sikerhez (Kumar et al., 2023).

Fritsch (2022, pp. 41–45) kutatásai szerint, az AI-k sokféleképpen felhasználhatók malware-ekben. Az AI elrejtheti a rosszindulatú programok kódját az észleléstől, elkerülheti a forgalom észlelést. Használhatják a védekező AI támadására, a mobil berendezéseken használt hitelesítési tényezők ellopására. Valamint az AI javíthatja az adathalászatot és az önállóan tanult kiber-fizikai szabotázszt.

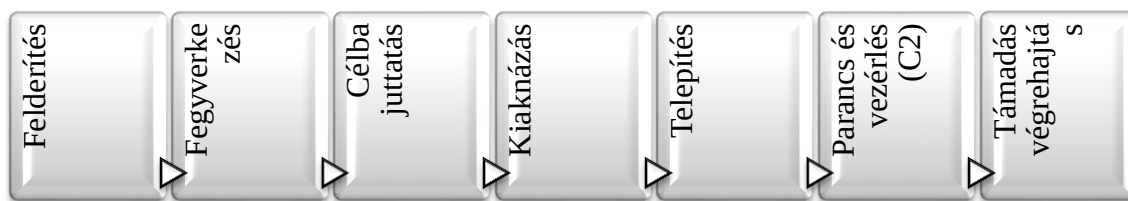
Ekképpen az AI segíthet az „intelligens” rosszindulatú programok létrehozásában, amelyek képesek tanulni a környezetből, amelybe beszivárognak, módosítani stratégiáit az észlelés elkerülése érdekében, és maximalizálni az általuk okozott károkat. Ez azt jelenti, hogy a hagyományos biztonsági védelem, például az aláírás-alapú malware-ek észlelése gyakran nem megfelelő ezekkel a fejlett fenyegetésekkel szemben (Kumar et al., 2023).

Guembe (2022) tanulmányában, 46 módszeresen kiválasztott tanulmányban azonosított négy jellemző AI-vezérelt támadási stratégiát: (1) Mély tanulás, (2) Biológiai ihletésű számítások (3) Rajintelligencia és (4) Fuzzy modell (Guembe et al., 2022).

5.1. Kiber Ölési Lánc

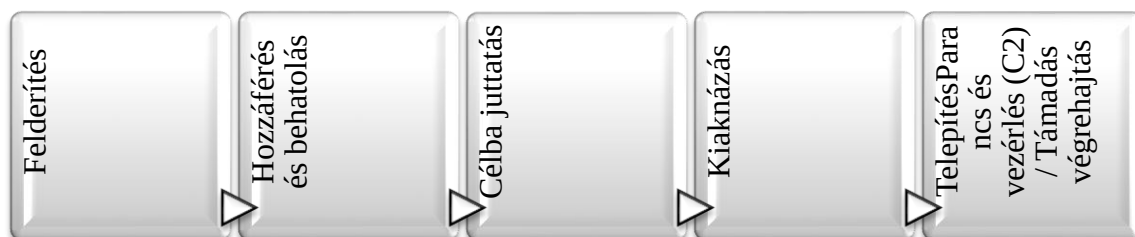
A Kiber Ölési Lánc (Cyber Kill Chain) egy olyan terv, ami lépésről lépésre mutatja be a kibertámadás folyamatát, az első felderítéstől a végső cél eléréséig. Ez a rendszer hasonló a behatolási teszteléshez (pentest), ami egy számítógépes rendszer elleni szimulált, engedélyezett támadást jelent, hogy értékeljék a rendszer biztonságát. A Cyber Kill Chain lépései segítenek a behatolástesztelőknek utánozni a rosszindulatú támadók stratégiáit, és feltárni a sebezhetőségeket minden fázisban. Ez a megközelítés lehetővé teszi a szervezetek számára, hogy teljes mértékben értékeljék védelmi intézkedéseiket, azonosítsák a gyengeségeket, és javítsák a biztonsági protokolljaikat. A Cyber Kill Chain gyakorlatilag egy ütemtervet ad a behatolási tesztelőknek, hogy rendszerezetten értékeljék a szervezet kibervédelmét (Zhao, 2024).

A Cyber Kill Chain lépéseit az 5. ábra mutatja be (Zhao, 2024).



ábra 5: Cyber Kill Chain. Saját szerkesztés

Guembe (2022) tanulmányában szisztematikusan elemzi az AI meghajtott támadások technikáit egy módosított Kiberbiztonsági Ölési Láncon. A módosított lánc lépéseit a 6. ábra mutatja (Guembe et al., 2022).



ábra 6: Módosított Cyber Kill Chain. Saját szerkesztés

5.2. AI meghajtott támadások a Kiber Ölési Láncon

5.2.1. Felderítési szakasz

A Cyber Kill Chain első lépése, a Felderítés, az információgyűjtés és az ellenfél infrastruktúrájának feltérképezésének fázisa. Az AI által vezérelt támadások ebben a szakaszban új dimenziót nyitnak meg, lehetővé téve az automatizált, nagy sebességű adatfeldolgozást és az adaptív, rugalmas válaszokat a változó környezetre (Zhao, 2024).

Módjai: Intelligens célprofilozás, Intelligens adatgyűjtés, Intelligens malware, Eredmény előrejelzés. Guembe (2022) tanulmányában ezeket a módokat részletezi.

5.2.2. Hozzáférés szakasz

A Cyber Kill Chain második fázisa, a Hozzáférés és behatolás, a támadók általi belépési pont meghatározásának és a rendszerbe történő behatolás folyamata. Az AI által vezérelt támadások ebben a szakaszban fokozzák a hatékonyságot és a sebességet, lehetővé téve a támadóknak, hogy gyorsan és észrevétlenül hatoljanak be a célszervezet hálózatába (Zhao, 2024).

Módjai: Automatizált adatforgalom-generálás/adathalászat (Bahnsen et al., 2018), AI-alapú jelszótalálgatás / jelszó feltörése (Hitaj et al., 2019; Lee & Yim, 2020; Trieu & Yang, 2018), Intelligens Captcha támadás és manipuláció (Li et al., 2021), Intelligens hamis értékelések generálása, AI modell manipuláció (Guembe et al., 2022).

5.2.3. Célba juttatás szakasz

A Cyber Kill Chain harmadik lépése, a Célba juttatás, a támadás célpontra irányításának szakasza. Az AI által irányított támadások ebben a szakaszban lehetővé teszik a precíz célpontra irányítást és a dinamikus reagálást a változó környezeti feltételekre, ezáltal maximalizálva a támadó sikerességét és minimalizálva az észlelés esélyét (Zhao, 2024).

Módja: Intelligens rejtőző és kitérő malware. A tanulmányban jelölt több idetartozó kutatásból hármat emelnék ki: (1) kifinomult adathalász URL létrehozás (Bahnsen et al., 2018), (2) észlelhetetlen malware programok generálása (Hu & Tan, 2017), (3) kifinomult kitérő malware (Kirat et al., 2018).

5.2.4. *Kiaknázás szakasz*

A Cyber Kill Chain negyedik lépése, a Kiaknázás, lehetővé teszi a támadónak, hogy kihasználja a megtalált sebezhetőségeket és behatoljon a célszervezet rendszerébe. Az AI által vezérelt támadások ebben a szakaszban optimalizálják a kiaknázási folyamatot, növelve annak hatékonyságát és gyorsaságát, miközben minimalizálják a felfedezés kockázatát (Zhao, 2024).

Módja: Viselkedéselemzés (Guembe et al., 2022; Petro & Morris, 2017).

5.2.5. *Parancs és vezérlés (C2) szakasz*

A Cyber Kill Chain hatodik lépése, a Parancs és vezérlés, a támadó infrastruktúrájának irányítása és ellenőrzése a cél eléréséhez. Az AI által irányított támadások ebben a szakaszban lehetővé teszik a támadó számára a gyors és adaptív reagálást a helyzetváltozásokra, maximalizálva a támadó hatékonyságát, sikerességét (Zhao, 2024).

Módjai: Intelligens öntanuló malwarek (Chung et al., 2019; Guembe et al., 2022), Automatizált domain generálás (Anderson et al., 2016; Guembe et al., 2022).

5.2.6. *Támadás végrehajtás szakasz*

A Cyber Kill Chain hetedik és utolsó lépése, a Támadás végrehajtás, a tervezett támadás végrehajtásának szakasza. Az AI által vezérelt támadások ebben a szakaszban lehetővé teszik a támadó számára a gyors és koordinált támadási műveleteket, maximalizálva a károkozás mértékét és minimalizálva a védelmi reakciók esélyét (Zhao, 2024).

Módja: AI-vezérelt DDoS támadás (Guembe et al., 2022).

6. GEN-AI HATÁSA A KIBERBIZTONSÁGRA DOSPERT ELEMZÉS

A primer kutatás során kérdőíves felmérés segítségével mértük fel, hogy a Gen-AI kiberbiztonságra való hatását mennyire tartják kockázatosnak a válaszadók, mennyire vállalják ezt a kockázatot és mennyi elvárt haszonnal számolnak. Ezen értékelésekből kockázati attitűd értékelést végeztünk a DOSPERT érték segítségével. Összes 290-en töltötték ki a kérdőívet, minden választ fel tudtunk használni a kiértékelés során.

6.1. Demográfia profil

Az összegyűjtött demográfiai adatokból láthatjuk (1. táblázat), hogy a kitöltők legnagyobb része felsőoktatást végzett (42.1%), 34.8%-uk gimnáziumot, fővárosban (46.6%), illetve városban él (31%). Legtöbbjük a 25 év alatti korcsoportba tartozik (46.6%) és nem IT (Információ és technológiai) területen dolgozik (85.9%). A kitöltők többsége nő volt (57.9%), bár ezen megoszlás kiegyensúlyozottnak mondható. Ezen szempont alapján következtetésem főleg a fiatalabb generációra, diplomával rendelkezőkre, és városban élőkre vonatkoztathatók.

N=290		fő	%			fő	%
Életkor	<25	135	46.6%	Lakhely	Falu	34	11.7%
	25 - <35	49	16.9%		Főváros	120	41.4%
	35 - <45	45	15.5%		Község	18	6.2%
	45 - <55	31	10.7%		Megyeszékhely	28	9.7%
	55 - <65	20	6.9%		Város	90	31.0%
	>65	10	3.4%		Total	290	100.0%
	Total	290	100.0%	Végzettség	Általános iskola	30	10.3%
Nem	Férfi	122	42.1%		Szakiskola	32	11.0%
	Nő	168	57.9%		Szakközépiskola	2	0.7%
	Total	290	100.0%		Gimnázium	101	34.8%
Foglalkozás	IT	41	14.1%		Technikum	1	0.3%
	Nem IT	249	85.9%		OKJ	2	0.7%
	Total	290	100.0%		Egyetem	122	42.1%
					Total	290	100%

táblázat 1: Demográfiai profil

6.2. DOSPERT elemzés

A Gen-AI kiberbiztonsági alkalmazásainak kockázatait vizsgáltam, és ennek fényében alkottam egy speciális DOSPERT kérdőívet. Céлом az volt, hogy feltárjam, hogyan ítélik meg az emberek a kockázatokat és az elvárt hasznót a Gen-AI kiberbiztonsági alkalmazások kapcsán. Az elemzésem által mélyebben megérthetjük az emberek hajlandóságát az ilyen technológiák

elfogadására és alkalmazására, valamint az ezzel járó kockázatokra és biztonsági aggályokra való reakciójukat.

6.2.1. Kockázatvállalási szándék

A kockázatvállalási szándék értékének meghatározásához a DOSPERT kérdőív kitöltőinek első részében olyan helyzeteket és állításokat kellett értékelniük, amelyek kockázatvállalással kapcsolatosak. Ezek a helyzetek általában leírják különböző tevékenységeket vagy döntési helyzeteket, és a résztvevőknek értékelniük kellett, mennyire lennének hajlandóak kockázatot vállalni az adott helyzetben. A válaszokat 1-7-ig terjedő skálán kellett megadniuk, ezzel kifejezve, milyen magas szándékkal vállalnának kockázatot az adott helyzetben.

Az egyes válaszokhoz rendelt pontok átlaga adja meg a résztvevő kockázatvállalási szándékának értékét az adott tényezők mentén. Minél magasabb a pontszám, annál nagyobb a kockázatvállalási szándék az adott szituációban. A kockázatvállalás értéke reprezentálja az egyéni kockázatvállalási szándékot és döntési mintázatokat az adott környezetben vagy helyzetben. Az eredményeket a 2. táblázat tartalmazza, a kérdőívben szereplő állítások a dolgozat mellékletében találhatók.

	N=290	Átlag	Me	Mó	s	Ferdeség	Cronbach α
Etikai	RT_1	3.49	3.5	4	1.759	0.140	0.823
	RT_2	2.94	3	1	1.668	0.472	
	RT_3	3.03	3	1	1.613	0.313	
	RT_4	2.32	2	1	1.531	1.016	
	RT_5	2.60	2	1	1.533	0.705	
	RT_6	2.61	2	1	1.692	0.847	
Pénzügyi	RT_7	2.65	2	1	1.645	0.792	0.853
	RT_8	2.96	3	1	1.721	0.545	
	RT_9	2.84	3	1	1.706	0.629	
	RT_10	2.87	3	1	1.782	0.596	
	RT_11	2.81	2	1	1.759	0.664	
	RT_12	2.85	3	1	1.706	0.612	
Egészségi és biztonsági	RT_13	2.42	2	1	1.656	1.093	0.867
	RT_14	2.24	2	1	1.564	1.125	
	RT_15	2.48	2	1	1.693	0.981	
	RT_16	2.72	2	1	1.670	0.687	
	RT_17	2.53	2	1	1.672	0.878	
	RT_18	2.62	2	1	1.725	0.810	
Szabadidő	RT_19	3.27	3	1	1.988	0.378	0.839
	RT_20	3.31	3	1	1.871	0.273	
	RT_21	3.94	4	4	1.923	-0.067	
	RT_22	2.95	3	1	1.868	0.483	
	RT_23	3.98	4	1	2.008	-0.098	
	RT_24	3.93	4	4	1.856	-0.005	

Közösségi	RT_25	3.96	4	5	1.806	-0.110	0.761
	RT_26	3.90	4	4	1.829	-0.095	
	RT_27	2.82	3	1	1.717	0.672	
	RT_28	3.57	4	3	1.810	0.157	
	RT_29	2.88	3	1	1.855	0.574	
	RT_30	2.93	3	1	1.757	0.502	

táblázat 2: Kockázat vállalási aspektusból megválaszolt kérdések eredményei

Az egyes alcsoportokhoz tartozó állítások megbízhatóságát Cronbach alpha mutatóval ellenőriztem, melyek alapján a kérdések megbízhatósága jónak mondható, mivel a Cronbach alpha értéke 0.75 felett értéket mutatott. A 3. táblázat a kérdéscsoportokhoz tartozó összesített Dospert értéket, illetve az összesített Cronbach alpha értéket mutatja.

Alskála	Összesített értékek
Etikai	2.832
Pénzügyi	2.828
Egészség és biztonság	2.502
Szabadidős	3.561
Közösségi	3.345
Cronbach α	0.939
DOSPERT érték	3.014

táblázat 3: Kockázat vállalási aspektusból megválaszolt kérdések csoportosított összesített eredményei

Az eredményeken látható, hogy a kockázatvállalási szándék elég alacsony, az 1-7-ig terjedő skálán a 290 kitöltő átlagosan 3.014 DOSPERT értéket ért el. A ferdeség értékeiből leolvasható, hogy az öt csoportból kettőnél több kérdésre is jellemzően magasabb pontokat adtak, amiből arra következtetek, hogy a kitöltők a szabadidős és közösségi csoportban szívesebben vállalnak kockázatot. Utóbbi következtetést alátámasztja a kapott összesített DOSPERT érték is, a szabadidős és közösségi csoportokban 3 feletti, míg a többiben 3 alatti ez az érték. Mindemellett a Cronbach-alfa magas (0.939) értéke biztosít arról, hogy a tesztkérdések nagyon összefüggenek egymással, egységesen mérnek, tehát a teszt megbízható volt.

6.2.2. Kockázátészlelés

A kockázátészlelés értékelése az egyik kulcsfontosságú lépés a kiberbiztonsági döntések meghozatalában, mivel lehetővé teszi a lehetséges veszélyek és fenyegetések azonosítását, valamint ezek valószínűségének és hatásának felmérését. A kockázátészlelés segítségével megállapítható, hogy mennyire veszélyesek bizonyos kiberbiztonsági incidensek, és milyen mértékben érintik az adott rendszert vagy szervezetet.

A DOSPERT módszer lehetőséget nyújt arra, hogy megértsük az emberek kockázatokban látott valószínűségét a különböző szituációkban. A kérdőív ezen részében a résztvevőknek azt kellett értékelniük, hogy mennyire tartják veszélyesnek az adott tevékenységet vagy döntési helyzetet.

Ebben a fejezetben a kockázateszlelés eredményeit vizsgálom a Gen-AI kiberbiztonsági alkalmazásainak kontextusában. A 4. táblázat a kapott eredményeket mutatja a Cronbach alpha megbízhatósági mutatóval együtt.

	n=290	Átlag	Me	Mó	s	Ferdeség	Cronbach α
Etikai	RP_1	3.95	4	4	1.698	-0.082	0.901
	RP_2	4.01	4	4	1.862	0.042	
	RP_3	3.81	4	3	1.836	0.073	
	RP_4	4.01	4	1a	2.041	-0.036	
	RP_5	4.02	4	7	2.052	-0.002	
	RP_6	4.04	4	1	2.138	-0.057	
Pénzügyi	RP_7	3.76	4	1	1.964	0.073	0.890
	RP_8	3.49	3	3	1.814	0.306	
	RP_9	3.50	4	1	1.855	0.153	
	RP_10	3.50	4	4	1.829	0.240	
	RP_11	3.80	4	4	1.849	0.002	
	RP_12	3.60	4	4	1.811	0.126	
Egészségi és biztonsági	RP_13	4.26	4	7	2.140	-0.161	0.945
	RP_14	4.22	4	7	2.246	-0.153	
	RP_15	4.18	4	7	2.102	-0.119	
	RP_16	4.29	4	7	2.111	-0.166	
	RP_17	4.10	4	7	2.123	-0.032	
	RP_18	4.17	4	7	2.136	-0.123	
Szabadidő	RP_19	3.23	3	1	1.913	0.419	0.847
	RP_20	3.57	3	4	1.820	0.310	
	RP_21	3.09	3	1	1.737	0.488	
	RP_22	3.00	3	1	1.710	0.534	
	RP_23	3.09	3	1	1.817	0.460	
	RP_24	3.11	3	1	1.718	0.342	
Közösségi	RP_25	3.50	3	3	1.703	0.184	0.797
	RP_26	3.91	4	4	1.761	-0.037	
	RP_27	3.23	3	4	1.667	0.324	
	RP_28	3.28	3	1	1.731	0.278	
	RP_29	3.52	4	1	1.950	0.156	
	RP_30	3.49	4	4	1.728	0.127	

táblázat 4: Kockázateszlelés eredményei

Az alcsoportokhoz tartozó Dospert értékeket az 5. táblázat összesíti, a megbízhatósági Cronbach alpha mutatóval együtt.

Alskála	Összesített értékek
Etikai	3.974
Pénzügyi	3.609
Egészség és biztonság	4.203
Szabadidős	3.183
Közösségi	3.487
Cronbach α	0.945
DOSPERT érték	3.691

táblázat 5: Kockázátészlelés csoportosított összesített eredményei

Az eredmények azt mutatják, hogy a kockázátészlelés jóval magasabb, mint a kockázatvállalási hajlandóság, az 1-7-ig terjedő skálán a 290 kitöltő átlagosan 3.691 DOSPERT értéket ért el. A ferdeség értékeiből leolvasható, hogy a kérdésekben jellemzően magas kockázatot észleltek, nagyon sok a negatív érték, és ha pozitív is, nagyon közel van a 0-hoz, ami azt jelenti, hogy magas pontokat adtak a válaszadók. Megfigyelhető, hogy a szabadidős kockázatoknál feltett kérdéseknél nincs negatív ferdeségi érték, tehát ezen szabadidős tevékenységekre vonatkozó állításoknál nem ítélték olyan kockázatosnak az AI hatását a kiberbiztonságra, mint amilyen kockázatosnak vélték az egészség és biztonság csoportban megadott állításokat. Utóbbi következtetést alátámasztja a kapott összesített DOSPERT érték is, a szabadidős csoportnak a legalacsonyabb, az egészség és biztonság csoportnak pedig a legmagasabb az összesített DOSPERT értéke. Mindemellett a Cronbach-alfa összesített (0.945), illetve alcsoportokra (>0.79) kapott magas értéke biztosít arról, hogy a tesztkérdések nagyon összefüggenek egymással, egységesen mérnek, tehát a teszt megbízható volt.

6.2.3. Elvárt haszon

Az elvárt haszon vizsgálata a végső lépés a kockázatvállalási döntések meghozatalában, mivel segít meghatározni, hogy egy adott kockázattal járó tevékenység vagy döntés milyen előnyökkel járhat. A kockázatvállalás gyakran összekapcsolódik az elvárt haszon értékelésével, mivel az emberek hajlandósága kockázatot vállalni jellemzően függ az esetleges jutalomtól vagy pozitív kimenettől.

A DOSPERT módszer ezen része lehetővé teszi, hogy megértsük az emberek elvárt haszon értékelési folyamatát különböző helyzetekben. Az állításokat a résztvevőknek az adott tevékenység vagy döntés lehetséges pozitív kimenetelének szempontjából kellett értékelniük.

Ebben a fejezetben az elvárt haszon eredményeit vizsgálom a Gen-AI kiberbiztonsági alkalmazásainak kontextusában. A 6. táblázat mutatja az állításokra kapott leíró statisztikai értékeket és a megbízhatósági értékeket.

	n=290	Átlag	Me	Mó	s	Ferdeség	Cronbach α
Etikai	EB_1	3.61	4	4	1.722	0.016	0.833
	EB_2	3.34	3	1	1.826	0.332	
	EB_3	3.05	3	1	1.692	0.399	
	EB_4	2.74	2	1	1.689	0.682	
	EB_5	2.71	2	1	1.614	0.746	
	EB_6	2.64	2	1	1.656	0.823	
Pénzügyi	EB_7	3.33	3	4	1.707	0.262	0.886
	EB_8	3.46	4	4	1.727	0.083	
	EB_9	3.37	3	3	1.705	0.174	
	EB_10	3.33	3	4	1.670	0.158	
	EB_11	3.17	3	1	1.683	0.271	
	EB_12	3.56	4	1	1.828	0.072	
Egészségi és biztonsági	EB_13	2.64	2	1	1.757	0.772	0.913
	EB_14	2.50	2	1	1.701	0.940	
	EB_15	2.59	2	1	1.711	0.821	
	EB_16	2.70	2	1	1.775	0.756	
	EB_17	2.60	2	1	1.700	0.840	
	EB_18	2.63	2	1	1.705	0.890	
Szabadidő	EB_19	4.14	4	4	1.973	-0.174	0.911
	EB_20	3.49	3	3	1.769	0.170	
	EB_21	4.24	5	5	1.948	-0.236	
	EB_22	4.07	4	4	1.911	-0.167	
	EB_23	4.22	4	4	1.947	-0.229	
	EB_24	4.24	4	4	1.932	-0.170	
Közösségi	EB_25	3.63	4	4	1.743	-0.026	0.831
	EB_26	3.65	4	4	1.768	0.055	
	EB_27	3.63	4	4	1.847	0.096	
	EB_28	3.66	4	4	1.690	-0.036	
	EB_29	3.55	3	1	1.888	0.162	
	EB_30	3.58	4	4	1.804	0.029	

táblázat 6: Elvárt haszon aspektusából megválaszolt kérdések eredményei

Az összesített alcsoportonkénti DOSPERT értéket a megbízhatósági mutatóval a 7. táblázat tartalmazza.

Alskála	Összesített értékek
Etikai	3.017
Pénzügyi	3.370

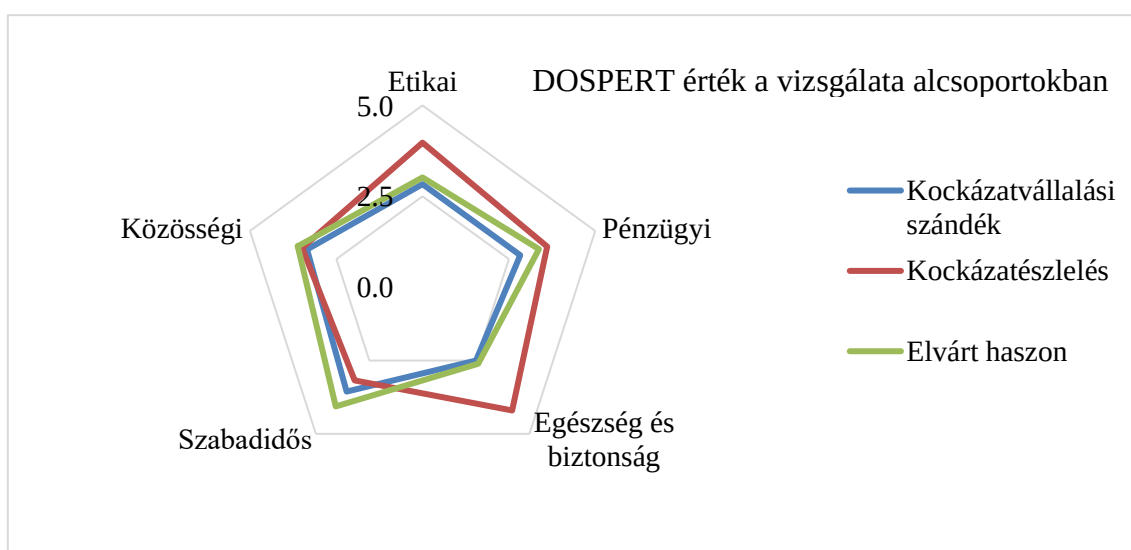
Egészség és biztonság	2.611
Szabadidős	4.066
Közösségi	3.616
Cronbach α	0.947
DOSPERT érték	3.336

táblázat 7: Elvárt haszon aspektusából megválaszolt kérdések csoportosított összesített eredményei

Az eredmények szerint, az elvárt haszon a kockázatvállalási szándék és a kockázateszlelés közé esik, az 1-7-ig terjedő skálán a 290 kitöltő átlagosan 3.336 DOSPERT értéket ért el. A ferdeség értékeiből leolvasható, hogy a kérdéseket jellemzően alacsony elvárt haszonnal értékelték. Megfigyelhető, hogy a szabadidős hasznoknál feltett kérdéseknél a legtöbb negatív ferdeségi érték, tehát ezen szabadidős tevékenységeket ítélték a legnagyobb elvárható haszonnal, míg az egészség és biztonság csoportba tartozó állításoknál magas ferdeségi értékeket látunk, tehát itt várták el a legkevesebb hasznot. Utóbbi következtetést alátámasztja a kapott összesített DOSPERT érték is, a szabadidős csoportnak a legmagasabb, az egészség és biztonság csoportnak pedig a legalacsonyabb. Mindemellett a csoportonkénti (>0.83) és az összesített (0.947) Cronbach-alfa magas értéke biztosít arról, hogy a tesztkérdések nagyon összefüggenek egymással, egységesen mérnek, tehát a teszt megbízható volt.

6.2.4. DOSPERT értékek az alcsoportokban

Az alcsoportok szerinti DOSPERT értékek összehasonlítása is érdekes eredményeket ad, melyek szemléltetése a 7. ábrán történik, illetve az értékek a 8. táblázatban találhatók.



ábra 7: DOSPERT értékek aspektusok szerint a vizsgált alcsoportokban radar diagram

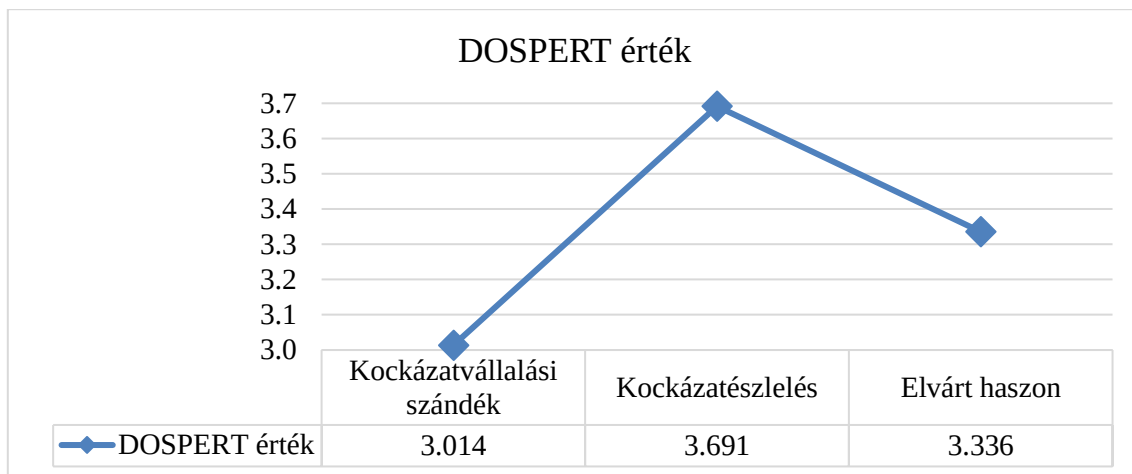
<i>Alskála</i>	<i>Kockázatvállalási szándék</i>	<i>Kockázatészlelés</i>	<i>Elvárt haszon</i>
Etikai	2.832	3.974	3.017
Pénzügyi	2.828	3.609	3.370
Egészség és biztonság	2.502	4.203	2.611
Szabadidős	3.561	3.183	4.066
Közösségi	3.345	3.487	3.616

táblázat 8: DOSPERT értékek aspektusok szerint alskálák szerint csoportosítva

Az értékekből és az ábráról is leolvasható, hogy a kitöltők kockázatészlelésre jellemzően magasabb pontokat adtak, kiváltképp az egészség és biztonság csoportban, ahol a Generatív AI kiberbiztonsági alkalmazását 4.203-as DOSPERT érték mellett, a kockázatvállalási szándék és az elvárt hasznot rendre csak 2.502 és 2.611-re értékelték. Érdekesség, hogy a közösségi csoportban nagyon közel vannak az értékek egymáshoz, tehát hasonlóan értékelték mind a három aspektust, továbbá, hogy a szabadidős csoportban a kockázatvállalási szándék és az elvárt haszon is magasabb értékelést kapott, mint ahogy a tevékenységek kockázatát észlelték, tehát, a kitöltők a szabadidős állításokat jellemzően alacsonyabb kockázatúnak ítélték, mint amilyen valószínűséggel a viselkedési minta szerint cselekedtek volna, és még ezeknél is magasabb hasznot vártak el ezektől a tevékenységektől.

6.2.5. DOSPERT érték összehasonlítás a három kockázati csoportban

A DOSPERT érték vagy pontszám a kérdőív kitöltése után számított összegzett eredmény, amely az egyén kockázatvállalási hajlandóságát és döntéshozatali preferenciáit tükrözi különböző élethelyzetekben és területeken. Az alacsonyabb értékek általában visszafogottabb kockázatvállalást jelentenek, míg a magasabb értékek azt sugallhatják, hogy az egyén hajlandó nagyobb kockázatot vállalni bizonyos helyzetekben. A 8. ábra a kockázatvállalási szándék (RT kérdések) a kockázatészlelés (RP kérdések) és az elvárt haszon (EB kérdések) összesített DOSPERT összehasonlítását mutatja.



ábra 8: DOSPERT értékek aspektusok szerint vonal diagram

Az átlagos kockázatvállalási szándék, kockázatészlelés és elvárt haszon értékelése mind mérsékelt szinten van az 1-7-ig terjedő skálán. A kockázatvállalás összesített DOSPERT értéke (közel 3,01) alacsonyabb, mint a skála közepén lévő érték (4), ami azt jelenti, hogy az emberek általánosságban az észlelt kockázat és az elvárt haszon mellett, kevésbé hajlandóak nagy kockázatot vállalni a Gen-AI kiberbiztonsági alkalmazásokkal kapcsolatban. A kockázatészlelés összesített DOSPERT értéke (közel 3,69) kissé magasabb, mint a kockázatvállalási szándék összesített DOSPERT értéke, ami azt jelzi, hogy az emberek inkább észlelik a kockázatokat a témában, mint ahogyan hajlandóak rájuk vállalkozni. Az elvárt haszon összesített DOSPERT értéke (közel 3,34) szintén közel van a skála közepéhez, ami azt jelzi, hogy az emberek átlagosan közepesen értékelik az elvárt hasznot, amit a Gen-AI kiberbiztonsági alkalmazások nyújthatnak.

A DOSPERT pontszámok azt jelzik, hogy az átlagos kockázatvállalási szándék és elvárt haszon értékelése közepes szinten van, míg a kockázat értékelése kicsit magasabb. Ez azt sugallja, hogy az emberek általában közepes mértékben hajlandóak kockázatot vállalni, és jobban észlelik a kockázatokat, de közepes mértékű hasznot várnak el a Gen-AI kiberbiztonsági alkalmazások kapcsán.

6.3. Kockázat attitűd vizsgálat

A DOSPERT skála szerinti kockázati attitűd vizsgálat regresszió segítségével számítható ki. Az SPSS-ben elvégzett regresszió számítás eredményével módunkban áll kiszámolni a Gen-AI kiberbiztonsági kockázataihoz való hozzáállást minden kérdésre, a kockázatészlelés és az elvárt haszon DOSPERT értékeivel súlyozva, az alábbi képlet segítségével.

$$Preferencia(X) = a(Elvart\ haszon(X)) + b(Kockazateszleles(X)) + c \quad (1)$$

Ahol az Expected Benefit az elvart haszon, a Perceived Risk pedig a kockázateszlelés. A regresszió során a függő változót a kockázatvállalási szándék (RT) kérdései adták. A kapott lineáris regressziós együtthatókat a 9. táblázat tartalmazza.

	Együtthatók
	B
c – (Konstans)	0.675
b – Kockázateszlelés DOSPERT PONT	-0.020
a – Elvart haszon DOSPERT PONT	0.723
Függő változó: Kockázatvállalási szándék DOSPERT PONT	

táblázat 9: DOSPERT értékek regresszió számítás részlet

A lineáris regressziós egyenes így a következő:

$$Preferencia(X) = 0.675 + 0.723 * (Elvart\ haszon(X)) - 0.02 * (Kockazateszleles(X)) \quad (2)$$

A negatív b együttható kockázat kerülő (risk aversion) magatartást jelez. Ezt láthatjuk a kockázat magatartás számított értékein is (Risk Attitude) (10. táblázat). Minden állítás esetén az érték 2 és 4 közé esik, amely értékek az 1-7 skála középső értékénél (4) kisebbek. Tehát a kitöltők kockázathoz való hozzáállása minden állítás esetében mérsékelt mértékben alacsonynak mondható, ami azt jelenti, hogy inkább hajlanak a kockázatkerülő magatartás felé. Ez azt jelzi, hogy általában inkább óvatosak és elővigyázatosak, amikor kockázatos helyzetekbe kerülnek, és inkább kerülnek azokat, amelyeknek potenciálisan negatív következményei lehetnek.

Alcsoport	Kérdés	Kockázateszlelés	Elvart haszon	Kockázati Magatartás
Etikai	1	3.95	3.61	3.207
	2	4.01	3.34	3.014
	3	3.81	3.05	2.803
	4	4.01	2.74	2.575
	5	4.02	2.71	2.558
	6	4.04	2.64	2.507
Pénzügyi	7	3.76	3.33	3.006
	8	3.49	3.46	3.109
	9	3.50	3.37	3.044
	10	3.50	3.33	3.012
	11	3.80	3.17	2.891
	12	3.60	3.56	3.176
Egészség és biztonság	13	4.26	2.64	2.503

	14	4.22	2.50	2.396
	15	4.18	2.59	2.467
	16	4.29	2.70	2.542
	17	4.10	2.60	2.476
	18	4.17	2.63	2.492
Szabadidős	19	3.23	4.14	3.603
	20	3.57	3.49	3.130
	21	3.09	4.24	3.678
	22	3.00	4.07	3.560
	23	3.09	4.22	3.663
	24	3.11	4.24	3.677
Közösségi	25	3.50	3.63	3.231
	26	3.91	3.65	3.238
	27	3.23	3.63	3.234
	28	3.28	3.66	3.253
	29	3.52	3.55	3.171
	30	3.49	3.58	3.194

táblázat 10: Kockázathoz való hozzáállás kérdésenként, alcsoportok szerint

6.3.1. DOSPERT pontok egyénenkénti korrelációja

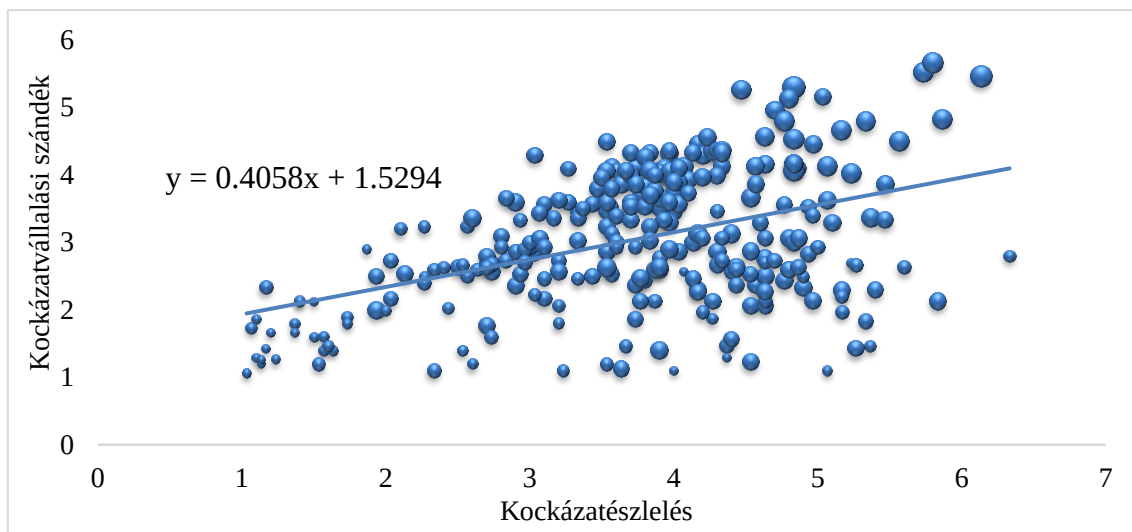
Következő lépésként megvizsgáltam, hogy milyen erős a kapcsolat a válaszadók esetén a három alcsoportra adott válaszok között. Ehhez korrelációt használtam, melynek értékei azt mutatják, hogy milyen erős kapcsolat van két változó között, ahol az érték -1 és 1 között lehet (11. táblázat).

	<i>Kockázatvállalási szándék</i>	<i>Kockázátészlelés</i>	<i>Elvárt haszon</i>
<i>Kockázatvállalási szándék</i>	1		
<i>Kockázátészlelés</i>	0.476749	1	
<i>Elvárt haszon</i>	0.747703	0.654586	1

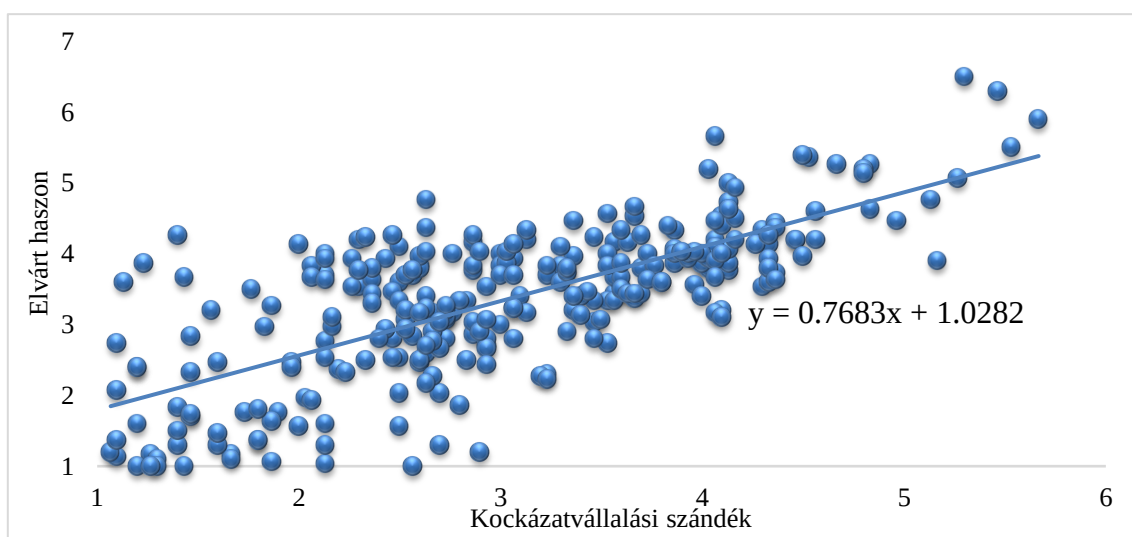
táblázat 11: DOSPERT pontok egyénenkénti korrelációja

- Kockázatvállalási szándék és kockázátészlelés: A 0.476749 érték erős pozitív korrelációt jelent. Ez azt jelzi, hogy azok, akik hajlandóak kockázatot vállalni, tendálnak arra, hogy kockázatosabban észleljék a kockázatot.
- Kockázatvállalási szándék és elvárt haszon: 0.747703 az érték, ami erős pozitív korrelációt jelent. Ez azt sugallja, hogy azok, akik hajlandóak nagyobb kockázatot vállalni, általában magasabb elvárt haszonnal számolnak.
- Kockázátészlelés és elvárt haszon: 0.654586 az érték, ami közepesen erős pozitív korrelációt jelent. Ez azt jelzi, hogy azok, akik kockázatosabban észlelik a kockázatot, általában magasabb elvárt haszonnal számolnak.

Az egyéni válaszadások esetén megfigyelhető lineáris regresszióval is a pozitív erős kapcsolat. A 9. és a 10. ábra a válaszadók esetén mutatja be a kockázateszlelés – kockázatvállalási szándék, és a kockázatvállalási szándék és elvárt haszon közötti kapcsolatot. Az ábrák a lineáris regresszió egyenletét is mutatják.



ábra 9: Kockázateszlelés és kockázatvállalási szándék DOSPERT pontjainak kapcsolatának buborék diagramja



ábra 10: Elvárt haszon és kockázatvállalási szándék DOSPERT pontjainak kapcsolatának buborék diagramja

6.3.2. Aspektusok közötti korreláció

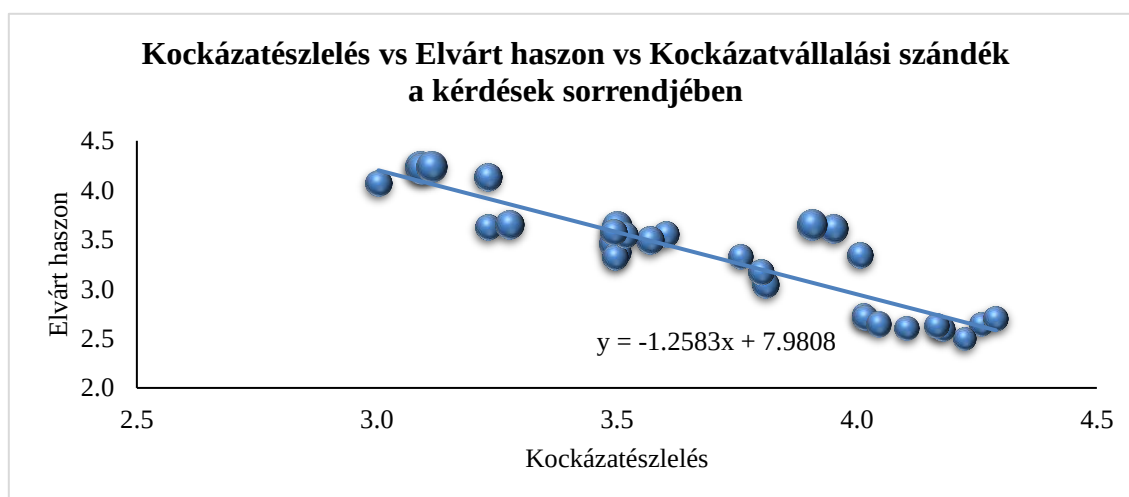
Érdekes megfigyelni, hogy ez egyes aspektusok közötti korreláció más trendet határoz meg a kérdések értékelésénél (12. táblázat).

	<i>Kockázátészlelés</i>	<i>Elvárt haszon</i>	<i>Kockázatvállalási szándék</i>
Kockázátészlelés	1		
Elvárt haszon	-0.907	1	
Kockázatvállalási szándék	-0.635	0.807	1

táblázat 12: Aspektusok közti korreláció

- Kockázátészlelés és elvárt haszon: Itt -0.907 a korreláció. Ez egy erős negatív korreláció, ami azt jelzi, hogy nagyobb kockázat esetén az elvárt haszon csökken. Ez azt sugallja, hogy általában az emberek hajlamosak lehetnek kevesebb hozamot elfogadni, ha magasabb a kockázat valószínűsége.
- Kockázátészlelés és kockázatvállalási szándék: -0.635 a korreláció értéke. Ez szintén egy negatív korreláció, bár kisebb, mint az előző esetben. Ez azt jelenti, hogy általában minél magasabb a kockázat észlelése, annál kevésbé hajlanak az emberek a kockázatvállalásra.
- Elvárt haszon és kockázatvállalási szándék: Itt 0.807 a korreláció értéke. Ez egy erős pozitív korreláció, ami azt sugallja, hogy az emberek általában nagyobb hasznot várnak el, ha hajlandóak nagyobb kockázatot vállalni.

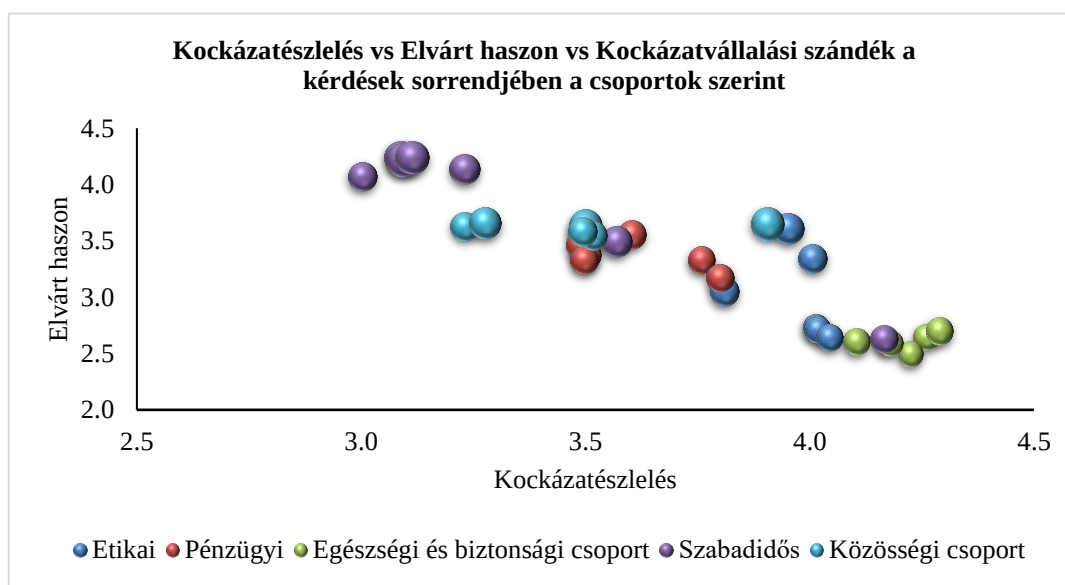
Ezen értékek segítségével látható, hogy hogyan kapcsolódnak egymáshoz a vizsgált változók, és milyen módon befolyásolják egymást a döntésekben vagy a viselkedésben. A három aspektus minden kérdésre vetített korrelációját a 11. ábra mutatja, mely tartalmazza a kockázat észlelése és az elvárt haszon közötti lineáris regressziós egyenes egyenletét is.



ábra 11: Aspektusok közti korreláció buborék diagramja

Megfigyelhető egy csökkenő trend, a kockázátészlelés növekedésével az elvárt haszon csökken, a kockázatvállalási szándék változik. Ez azt jelenti, hogy minél nagyobb a kockázat, annál

kevesebb hasznot várnak. Ez logikus, mivel a nagyobb kockázatok gyakran nagyobb bizonytalansággal járnak, ami csökkenti a potenciális hasznot. A 12. ábra csoportokra bontva mutatja be ezen kapcsolatot, így látható, hogy az alcsoportokra kapott válaszok alapján a kapott értékek más-más biztonsági besorolásba kerültek a válaszadók szerint. A legkisebb kockázati észlelés a szabadidős csoportban volt, de ott a legnagyobb az elvárt haszon, míg a legnagyobb észlelési értékek az egészség és biztonság kérdéseinél párosultak a legkisebb haszonnal.



ábra 12: Aspektusok közti korreláció a vizsgált csoportok szerint buborék diagram

6.3.2.1. DOSPERT érték vizsgálata lakhely szerint

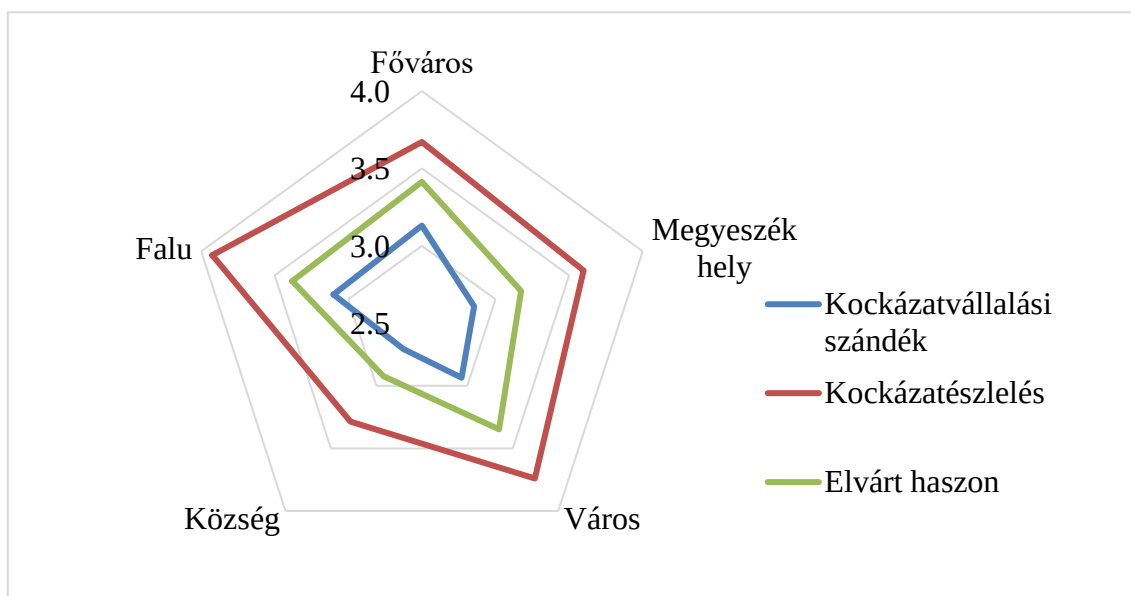
A három kockázathoz kapcsolódó kérdéseket néhány demográfiai változó esetén külön vizsgáltam. A lakhely szerint nem találtam szignifikáns különbséget, bár a minta a főváros és a város irányában torzít (13. táblázat).

	F	Sig.
Kockázatvállalási szándák	1.098	0.358
Kockázatészlelés	0.950	0.436
Elvárt haszon	0.930	0.447

táblázat 13: DOSPERT pontok aspektusonként ANOVA teszt eredménye

A lakhely szerinti vizsgálathoz a DOSPERT értékekkel ANOVA tesztet futtattam le SPSS rendszerben. A szignifikancia értékekből látható, hogy a lakóhely viszonylatában nincs különbség a kapott DOSPERT pontokban, mert mindegyik szignifikancia érték nagyobb mint 5% (0.05).

A 13. ábrán látható, hogy általánosságban minden településen a kockázat észlelése magasabb, mint az elvárt haszon, és hogy a kockázatvállalási szándék a legkisebb. Érdekes, hogy falun a legmagasabb a kockázatészlelés, mégis hasonló a kockázatvállalási szándék és elvárt haszon, mint a fővárosban. Ennek oka lehet a technológia fiatalossága, illetve az elérhető edukáció limitáltsága is.



ábra 13: DOSPERT pontok aspektusok szerint lakhelyenként radar diagram

6.3.2.2. DOSPERT érték vizsgálata foglalkozási terület szerint

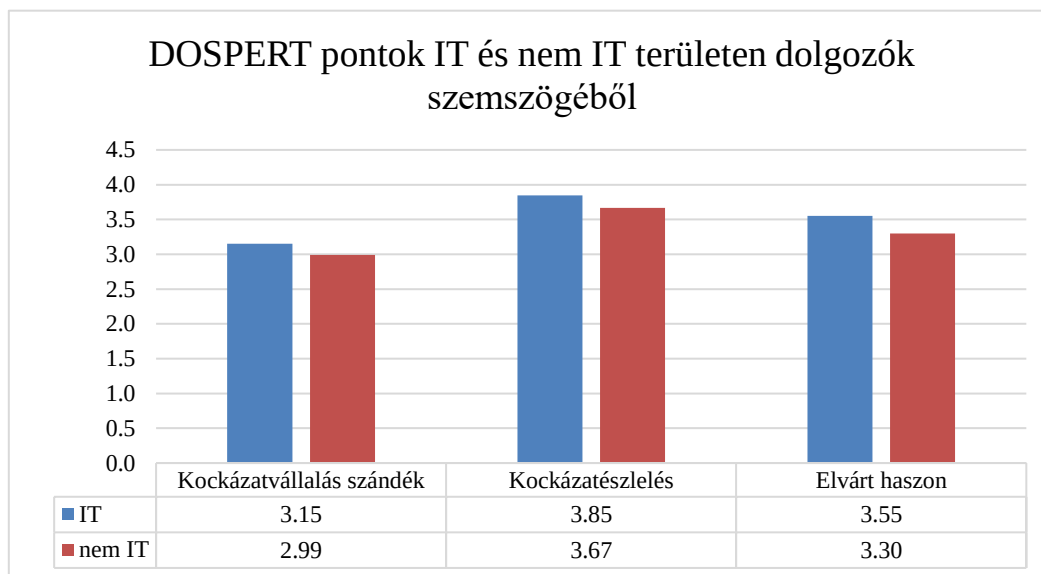
A foglalkozási területet két részre bontottam, itt kíváncsi voltam a Gen-AI kiberbiztonsági kockázatainak megítélésére olyan emberek véleménye szerint, akik IT (Információ és technológia) és akik nem IT területen dolgoznak. Az eredményeket a DOSPERT értékekkel futtatott kétmintás t-próbával kaptam meg SPSS rendszerben (14. táblázat). Mivel a szórásazonosságok nem egyeztek meg, így a nem egyenlő szórásazonosságra vonatkozó eredményeket vizsgáltam.

	t	df	Sig. (2-tailed)
Kockázatvállalási szándék	1.168	68.994	0.247
Kockázatészlelés	1.100	64.816	0.276
Elvárt haszon	1.531	60.732	0.131

táblázat 14: DOSPERT pontok aspektusonként két mintás t-teszt eredménye

Ennél a tesztnél is azt vizsgálhatjuk meg, hogy a foglalkozási terület nem befolyásolja a kapott eredményeket. Tehát az eredmények értelmében nem volt szignifikáns különbség, hogy a

kitöltő IT-s volt vagy sem. Ezt az eredményt torzíthatja az, hogy a válaszadók mindössze 14%-a dolgozik IT területen. A 14. ábra grafikusan mutatja be a két területen dolgozók eredményeit.



ábra 14: DOSPERT pontok aspektusonként IT és nem IT területen dolgozók szemszögéből csoportosított oszlop diagram

Megfigyelhető, hogyha nem is sokkal, de magasabb DOSPERT értéket értek el mind a három aspektusban az IT területen foglalkozók, ami arra enged következtetni, hogy az IT-s emberek véleménye nem tér el jelentős mértékben a többiekétől, annak ellenére, hogy olyan területen dolgoznak, ami szorosan kapcsolódik a dolgozat témájához.

6.4. Következtetések

Az elemzés során azt állapítottam meg, hogy az átlagos kockázatvállalási szándék, kockázateszlelés és elvárt haszon értékelése közepesen alacsony szinten van az 1-7-ig terjedő skálán. Általánosságban elmondható, hogy az emberek magasabban észlelik a kockázatokat, mint ahogyan hajlandóak rájuk vállalkozni, és a kettő között értékelik az elvárt hasznót a Gen-AI kiberbiztonsági alkalmazásokkal kapcsolatban.

Az al csoportok elemzése során azt tapasztaltam, hogy bizonyos területeken, például az egészség és biztonság terén, alacsonyabbak az elvárt haszon értékelések, ami arra utal, hogy az emberek kevésbé látják az előnyöket ezen a területen. Ugyanakkor a szabadidős tevékenységek esetében magasabb elvárt haszon értékelésekkel találkoztam, ami azt jelzi, hogy ezen területeken nagyobb várakozással tekintenek az emberek a Gen-AI alkalmazásokra.

A DOSPERT értékek regressziója további érdekes következtetéseket kínált számomra. Az eredmények alapján általánosságban inkább a kockázatkerülő magatartás felé hajlanak az emberek, azaz inkább óvatosak és elővigyázatosak kockázatos helyzetekben. Ennek ellenére vannak olyan területek, például a szabadidős tevékenységek, ahol magasabb a kockázatvállalási szándék, valószínűleg a nagyobb elvárt haszon miatt.

7. ÖSSZEFOGLALÁS

A dolgozat célja az volt, hogy áttekintést nyújtson a generatív mesterséges intelligencia (Gen-AI) kiberbiztonsági kockázatairól és lehetséges hatásairól. Az elemzés során különös figyelmet fordítottam a Gen-AI technológiák, például a generatív versengő hálózatok (GAN) és a deepfake modellek által felvetett kihívásokra, valamint azokra a módszerekre és eszközökre, amelyekkel ezeket a kockázatokat kezelni lehet.

A dolgozatban bemutatásra került, hogy a Gen-AI hogyan válhat potenciális eszközzé a kiberbűnözők és támadók számára különböző kiberbűncselekmények elkövetésére, például hamisított média létrehozására vagy akár adatlopásra és személyazonosság-lopásra. Az elemzés során kiemeltem a kiberbiztonsági védekezés fontosságát és az ehhez szükséges intézkedéseket, beleértve az AI-alapú védelmi mechanizmusok és detektálási módszerek fejlesztését.

Az általam vizsgált DOSPERT elemzés rávilágított arra, hogy az egyének kockázatértékelési hajlandósága jelentős mértékben befolyásolja az AI által generált kiberbiztonsági kockázatokkal szembeni attitűdöt és védekezési stratégiákat. Ezért kiemelt fontosságú a kiberbiztonsági tudatosság növelése és az egyének felkészítése a Gen-AI által felvetett kockázatok kezelésére.

Végül, a dolgozat rámutatott arra, hogy a Gen-AI technológiákban rejlő kiberbiztonsági kockázatok komplex és folyamatosan változó jellegűek, ezért az ezekre adott válaszoknak is dinamikusnak kell lenniük. Az AI-alapú kiberbiztonsági megoldások és politikák folyamatos fejlesztése és alkalmazása elengedhetetlen ahhoz, hogy lépést lehessen tartani lehetséges támadásokkal szemben, és biztosítani lehessen az online tér biztonságát és integritását.

IRODALOMJEGYZÉK

- Anderson, H. S., Woodbridge, J., & Filar, B. (2016). *DeepDGA: Adversarially-Tuned Domain Generation and Detection* (arXiv:1610.01969). arXiv. <http://arxiv.org/abs/1610.01969>
- Bahnsen, A. C., Torroledo, I., Camacho, L. D., & Villegas, S. (2018). *DeepPhish: Simulating Malicious AI*.
- Blais, A.-R., & Weber, E. U. (2006). A Domain-Specific Risk-Taking (DOSPERT) scale for adult populations. *Judgment and Decision Making*, 1(1), 33–47. <https://doi.org/10.1017/S1930297500000334>
- Chowdhury, M. M., Rifat, N., Ahsan, M., Latif, S., Gomes, R., & Rahman, M. S. (2023). ChatGPT: A Threat Against the CIA Triad of Cyber Security. *2023 IEEE International Conference on Electro Information Technology (eIT)*, 1–6. <https://doi.org/10.1109/eIT57321.2023.10187355>
- Chung, K., Kalbarczyk, Z. T., & Iyer, R. K. (2019). Availability attacks on computing systems through alteration of environmental control: Smart malware approach. *Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems*, 1–12. <https://doi.org/10.1145/3302509.3311041>
- Creswell, A., White, T., Dumoulin, V., Arulkumaran, K., Sengupta, B., & Bharath, A. A. (2018). Generative Adversarial Networks: An Overview. *IEEE Signal Processing Magazine*, 35(1), 53–65. <https://doi.org/10.1109/MSP.2017.2765202>
- Ekler, P., & Pásztor, D. (2020). Alkalmazott mesterséges intelligencia felhasználási területei és biztonsági kérdései – Mesterséges intelligencia a gyakorlatban. *Scientia et Securitas*, 1(1), 35–42. <https://doi.org/10.1556/112.2020.00006>
- Fritsch, L., Jaber, A., & Yazidi, A. (2022). An Overview of Artificial Intelligence Used in Malware. In E. Zouganeli, A. Yazidi, G. Mello, & P. Lind (Eds.), *Nordic Artificial Intelligence Research and Development* (Vol. 1650, pp. 41–51). Springer International Publishing. https://doi.org/10.1007/978-3-031-17030-0_4
- Gordon, C. (2023). *How General AI Will Eventually Reshape Everything*. Forbes. <https://www.forbes.com/sites/cindygordon/2023/09/30/how-general-ai-will-eventually-reshape-everything/?sh=5867ec7242cd>
- Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Applied Artificial Intelligence*, 36(1), 2037254. <https://doi.org/10.1080/08839514.2022.2037254>
- Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. *IEEE Access*, 11, 80218–80245. <https://doi.org/10.1109/ACCESS.2023.3300381>
- Hitaj, B., Gasti, P., Ateniese, G., & Perez-Cruz, F. (2019). PassGAN: A Deep Learning Approach for Password Guessing. In R. H. Deng, V. Gauthier-Umaña, M. Ochoa, & M. Yung (Eds.), *Applied Cryptography and Network Security* (Vol. 11464, pp. 217–237). Springer International Publishing. https://doi.org/10.1007/978-3-030-21568-2_11
- Hu, W., & Tan, Y. (2017). *Generating Adversarial Malware Examples for Black-Box Attacks Based on GAN* (arXiv:1702.05983). arXiv. <http://arxiv.org/abs/1702.05983>
- Jaggia, S., Kelly, A., Lertwachara, K., & Chen, L. (2023). *Business analytics: Communicating with numbers* (Second edition). McGraw Hill LLC.
- Kalota, F. (2024). A Primer on Generative Artificial Intelligence. *Education Sciences*, 14(2), 172. <https://doi.org/10.3390/educsci14020172>
- Kinicki, A., & Soignet, D. B. (2022). *Management: A practical introduction* (Tenth edition). McGraw-Hill Education.

- Kirat, D., Jang, J., & Stoecklin, M. (2018). *DeepLocker concealing targeted attacks with AI locksmithing*. <https://www.blackhat.com/us-18/briefings/schedule/index.html#deeplocker—concealing-targeted-attacks-with-ailocksmithing-11549>
- Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era. *Journal of Computers, Mechanical and Management*, 2(3), 31–42. <https://doi.org/10.57159/gadl.jcmm.2.3.23064>
- Lee, K., & Yim, K. (2020). Cybersecurity Threats Based on Machine Learning-Based Offensive Technique for Password Authentication. *Applied Sciences*, 10(4), 1286. <https://doi.org/10.3390/app10041286>
- Li, C., Chen, X., Wang, H., Wang, P., Zhang, Y., & Wang, W. (2021). End-to-end attack on text-based CAPTCHAs based on cycle-consistent generative adversarial network. *Neurocomputing*, 433, 223–236. <https://doi.org/10.1016/j.neucom.2020.11.057>
- Mallick, A. I., & Nath, R. (2024). *Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments*. <https://www.researchgate.net/publication/378343830>
- Petro, D., & Morris, B. (2017). *Weaponizing Machine Learning: Humanity Was Overrated Anyway*. DEF CON. <https://defcon.org/html/defcon-25/dc-25-speakers.html#Petro>
- Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cybersecurity. In A. Refsdal, B. Solhaug, & K. Stølen, *Cyber-Risk Management* (pp. 29–32). Springer International Publishing. https://doi.org/10.1007/978-3-319-23570-7_4
- Russell, S. J., Norvig, P., & Chang, M. (2021). *Artificial Intelligence: A modern approach* (Fourth edition, global edition). Pearson.
- Tick, A. (2023). Evaluation of Industry 4.0 familiarity at SMEs in Central-Eastern Europe using Machine Learning Algorithms. *2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 000643–000648. <https://doi.org/10.1109/SACI58269.2023.10158645>
- Trieu, K., & Yang, Y. (2018). *Artificial Intelligence-Based Password Brute Force Attacks*. <https://aisel.aisnet.org/mwais2018/39>
- Vähäkainu, P., & Lehto, M. (2019). *Artificial intelligence in the cyber security environment*.
- Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review*, 9(11), 39–52. <https://doi.org/10.22215/timreview/1282>
- Zhao, L. (2024). Navigating the Cyber Kill Chain: A modern approach to pentesting. *Applied and Computational Engineering*, 38(1), 170–175. <https://doi.org/10.54254/2755-2721/38/20230549>

MELLÉKLETEK

DOSPERT kérdőív kódolással

Risk Taking	Risk Perception	Expected Benefit	Sorszám	Kérdés
RT_1	RP_1	EB_1	1	” Ha IT területen dolgoznék, munkám során szívesen fejlesztenék GMI-algoritmusokat annak ellenére, hogy tudom, hogy ezek a technológiák alkalmasak lehetnek mind védekező, mind támadó kiberműveletekre.
RT_2	RP_2	EB_2	2	” Ha IT területen dolgoznék, munkám során együttműködnék MI-kutatókkal, miközben nem veszem figyelembe a GMI-technológiák lehetséges etikai következményeit és kockázatait a kiberbiztonság terén.
RT_3	RP_3	EB_3	3	” Munkámban és magánéletemben is használnék GMI-t annak ellenére, hogy tudom, ez lehetővé tesz olyan kifinomult adathalász támadásokat, amelyek veszélyeztethetik az egyének személyes adatait.
RT_4	RP_4	EB_4	4	” Ha IT területen dolgoznék, munkám során megfelelő biztosítékok nélkül osztanék meg GMI modelleket, annak ellenére, hogy ez lehetőséget adhat a rosszindulatú szereplőknek a kiberbiztonsági rendszerek sebezhetőségeinek kihasználására.
RT_5	RP_5	EB_5	5	” A felfedezett sebezhetőségek felelősségteljes feltárására vonatkozó egyértelmű iránymutatások nélkül használnék GMI-megoldásokat (céges vagy privát környezetben is), kockáztatva a kritikus rendszerek potenciális fenyegetéseknek való kitettségét.
RT_6	RP_6	EB_6	6	” Ha IT területen dolgoznék, munkám során nem foglalkoznék etikai megfontolásokkal a kiberbiztonsági GMI fejlesztése és alkalmazása során, annak ellenére, hogy ez nem kívánt

				következményekhez és károkhoz vezethet.
RT_7	RP_7	EB_7	7	” Befektetném az éves költségvetésemnek jelentős részét kiberbiztonsági megoldásokba, előre biztosítva a kibertámadásokból eredő esetleges pénzügyi veszteségeket.
RT_8	RP_8	EB_8	8	” Személyes vagy szervezeti vagyon védelme érdekében felosztanám pénzügyi forrásaim egy részét a legmodernebb kiberbiztonsági technológiákba való befektetésre.
RT_9	RP_9	EB_9	9	” Hozzájárulnék költségvetésem jelentős részével a kiberbiztonsági kutatás és fejlesztés támogatásához, hangsúlyozva a digitális védelemben történő megelőző befektetések fontosságát.
RT_10	RP_10	EB_10	10	” Fogadnék egy napi bevétellemmel egy kiberbiztonsági figyelemfelkeltő kampány sikerére, hogy az jelentősen csökkenti az adathalász támadások valószínűségét.
RT_11	RP_11	EB_11	11	” Fogadnék pénzügyi forrásaim egy részével egy kiberbiztonsági startup sikerére, azon spekulálva, hogy képes-e innovatív megoldásokat bevezetni a felmerülő fenyegetések leküzdésére.
RT_12	RP_12	EB_12	12	” Részt vennék egy kiberbiztonsági előrejelzési csoportban úgy, hogy egy napi bevételtem a következő nagyobb kiberfenyegetés vagy sebezhetőség pontos előrejelzésére teszek.
RT_13	RP_13	EB_13	13	” Megfelelő ellenőrzés nélkül töltenék le és használnék kiberbiztonsági eszközöket nem ellenőrzött forrásokból, ami potenciálisan rosszindulatú programoknak vagy sebezhetőségeknek teszi ki a rendszeremet.
RT_14	RP_14	EB_14	14	” Biztonságos csatornák vagy titkosítás használata nélkül osztanék meg érzékeny személyes adatokat online, ami az illetéktelen hozzáférést és az adatvédelem megsértését kockáztatja a kibertérben.
RT_15	RP_15	EB_15	15	” Az alapvető kiberbiztonsági gyakorlatok – például erős jelszavak vagy többlépcsős hitelesítés –

				alkalmazását elhanyagolnám, annak ellenére, hogy így digitális eszközeim potenciális jogosulatlan hozzáférésnek vannak kitéve.
RT_16	RP_16	EB_16	16	” Letiltanék vagy elhanyagolnék víruskereső szoftvereket és egyéb biztonsági intézkedéseket az eszközeimen, annak ellenére, hogy tudom, hogy ez veszélyezteti digitális környezetem általános biztonságát.
RT_17	RP_17	EB_17	17	” Kockázatos online magatartást tanúsítanék a megfelelő kiberbiztonsági tudatosság nélkül, amivel potenciálisan adathalász csalások vagy egyéb kiberfenyegetések áldozatává válnék.
RT_18	RP_18	EB_18	18	” Figyelmen kívül hagynám a lehetséges kiberfenyegetésekre vonatkozó figyelmeztetéseket, és folytatnám a kockázatos online tevékenységeket, ami veszélyezteti digitális identitásom és információim biztonságát.
RT_19	RP_19	EB_19	19	” Élő hacker kihívásban vennék részt, hogy ellenőrzött környezetben teszteljem kiberbiztonsági készségeimet.
RT_20	RP_20	EB_20	20	” Megpróbálnám kihasználni a biztonsági réseket egy olyan szimulált kiberbiztonsági környezetben, ami magasabb szintű készségeket követel, mint amivel jelenleg rendelkezem, de ezen szeretnék tanulással fejleszteni a szabadidőmben.
RT_21	RP_21	EB_21	21	” Részt vennék egy valós idejű kiberbiztonsági szimulációban, hogy megtapasztaljam a kifinomult kiberfenyegetésekkel szembeni védekezés kihívásait.
RT_22	RP_22	EB_22	22	” Jelentkeznék egy Capture The Flag (CTF) kiberbiztonsági versenyre, amellyel tesztelhetem és javíthatom a biztonsági kihívások észlelésének és megoldásának képességét.
RT_23	RP_23	EB_23	23	” Csatlakoznék egy hackelés témájú szabadulószoftver-tevékenységhez, ami szimulálja a kiberbiztonsági rejtélyek feltárásának és megoldásának élményét.
RT_24	RP_24	EB_24	24	” Részt vennék olyan programokban, ahol felfedezhetném az etikus hackelést

				a digitális rendszerek sebezhetőségeinek felelősségteljes azonosítása és jelentése érdekében.
RT_25	RP_25	EB_25	25	” Munkahelyemen kifejezném az aggodalmamat egy projekttel kapcsolatos potenciális GMI általi kiberbiztonsági kockázatokra nézve, még akkor is, ha ez ellenkezik a csapat uralkodó véleményével.
RT_26	RP_26	EB_26	26	” Kifejezném egyet nem értésemet a felettesem azon döntésével, hogy egy szoftverfejlesztési projektben előnyben részesítsem a funkciókat a biztonsággal szemben.
RT_27	RP_27	EB_27	27	” GMI elleni kiberbiztonsági kutatásra és fejlesztésre szakosodnék, mert ez összhangban van a szenvedélyemmel, még akkor is, ha más, tekintélyesebb karrierlehetőségek állnak rendelkezésre.
RT_28	RP_28	EB_28	28	” Kifejezném az GMI elleni kiberbiztonság fontosságával kapcsolatos nézőpontomat technológiáról és innovációról folytatott beszélgetések során társadalmi vagy szakmai körökben.
RT_29	RP_29	EB_29	29	” Elfogadnék egy állásajánlatot egy kiberbiztonsági központban, még akkor is, ha az azt jelenti, hogy távol kell költözni jelenlegi közösségi és családi köreimtől.
RT_30	RP_30	EB_30	30	” Harmincas éveim közepén átváltanék egy kiberbiztonsággal kapcsolatos szerepkörbe, és megmutatnám, hogy elkötelezett vagyok egy olyan területen, amely ismeretlen lehet jelenlegi társadalmi és szakmai köreim számára.