HADMÉRNÖK
VÉDELEMINFORMATIKA
21. évfolyam (2026) 3. szám 5–19.
DOI: 10.32567/hm.2026.3.1

Farkas Athéné[1]

A mesterséges intelligencia alkalmazási lehetőségei a kiberbiztonsági auditok gyakorlatában

Application Possibilities of Artificial Intelligence in the Practice of Cybersecurity Audits

Absztrakt

A kiberbiztonság napjainkra stratégiai jelentőségűvé vált a kritikus infrastruktúrák védelmében, amit a 2024. évi LXIX. törvény és annak kapcsolódó rendeletei is megerősítenek a NIST SP 800-53 Rev. 5-re épülő védelmi intézkedéskatalógus bevezetésével. A növekvő számú és összetettségű auditok jelentős erőforrásigénnyel járnak, ezért szükségessé válik a NIS2-nek való megfeleléshez végzett hazai kiberbiztonsági auditfolyamatok automatizálási lehetőségeinek vizsgálata. E tanulmány kifejezetten az alap biztonsági osztályba sorolt elektronikus információs rendszerekhez rendelt 164 védelmi intézkedéshez kapcsolódó auditbizonyítékok mesterségesintelligencia- (MI-)alapú feldolgozhatóságát vizsgálja, a hazai NIS2 auditmódszertanra építve. Újszerű eleme az auditbizonyítékok T1–T7 szerinti tipizálása, amely három dimenzió – a vizsgálati típus, a bizonyíték formátuma, az alkalmazható MI-technológia – összekapcsolásával rendszerezi az evidenciákat. A tipológia lehetővé teszi az egyes bizonyítéktípusok MI-szempontú minősítését, és kijelöli azokat a területeket, ahol reális a részleges vagy jelentősebb automatizálás. Az eredmények rámutatnak arra, hogy a szövegalapú, strukturált nyelvezetű dokumentumok ismétlődő mintázataik és sablonszerű megfogalmazásaik miatt alkalmasak természetesnyelv-feldolgozási technológiák alkalmazására, míg a képi vagy nem strukturált formátumú auditbizonyítékok – például képernyőképek, szkennelt dokumentumok – feldolgozásához

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Műszaki Doktori Iskola, e-mail: athene.farkas@proton.me

az optikai karakterfelismerés és a számítógépes látás integrációja szükséges. A tanulmány megállapítja, hogy a kiberbiztonsági auditok részleges automatizálása nem valósítható meg kizárólag szövegalapú mesterségesintelligencia-eszközökkel: hatékony auditautomatizáláshoz multimodális megközelítés szükséges, amely a természetesnyelv-feldolgozás mellett képfeldolgozó technológiákat is alkalmaz.

Kulcsszavak: kiberbiztonság, NIS2, audit, mesterséges intelligencia

Abstract

Cybersecurity has become a factor of strategic importance in the protection of critical infrastructures, a development reinforced by Act LXIX of 2024 and its implementing decrees through the introduction of a catalogue of security controls based on NIST SP 800-53 Rev. 5. The increasing number and complexity of audits require significant resources, which makes it necessary to examine the possibilities for automating national cybersecurity audit processes aimed at NIS2 compliance. The study specifically investigates the artificial intelligence (AI)-based processability of audit evidence associated with the 164 security controls assigned to electronic information systems classified in the basic security category, building on the national NIS2 audit methodology. A novel element of the study is the classification of audit evidence into types T1–T7, which systematises the evidence by linking three dimensions: type of examination, format of evidence, and applicable AI technology. This typology enables the AI-oriented evaluation of different types of evidence and identifies the areas where partial or more substantial automation is realistic. The results show that text-based documents with structured language are suitable for the application of natural language processing technologies due to their recurring patterns and template-like formulations, while the processing of image-based or unstructured audit evidence – such as screenshots and scanned documents – requires the integration of optical character recognition and computer vision. The study concludes that the partial automation of cybersecurity audits cannot be achieved solely with text-based artificial intelligence tools; effective audit automation requires a multimodal approach that, in addition to natural language processing, also applies image processing technologies.

Keywords: cybersecurity, NIS2, audit, artificial intelligence

Bevezetés

A kiberbiztonság az elmúlt években a kritikus infrastruktúrák védelmének egyik kulcstényezőjévé vált. Az ezeket érő kibertámadások közvetlenül veszélyeztethetik a társadalom működőképességét és az alapvető szolgáltatások folyamatosságát. Az Európai Unió NIS2 irányelve,[2] valamint annak hazai átültetése – különösen a 2024. évi LXIX. törvény Magyarország kiberbiztonságáról és az ehhez kapcsolódó végrehajtási rendeletek – érdemben szigorították a kiberbiztonsági követelményeket. Szélesebb

[2] Az Európai Parlament és a Tanács 2022/2555 irányelve.

szervezeti kört vontak be a szabályozás hatálya alá, és kötelezővé tették a rendszeres kiberbiztonsági auditokat a kritikus és fontos ágazatok szereplőinél.

Ezzel párhuzamosan a hazai jogszabályi környezet a NIST SP 800-53 Rev. 5[3] nemzetközi ajánlásra épülő védelmi intézkedéskatalógust alkalmazza. Az erre épülő NIST SP 800-53A Rev. 5[4] ellenőrzési módszertan rendkívül részletes, elemikövetelmény-szintű vizsgálatokat igényel. A megfelelési kötelezettségek bővülése, az auditált szervezetek számának növekedése és a kontrollkészletek komplexitása együtt azt eredményezik, hogy a hagyományos, manuális auditálási eljárások egyre inkább idő- és erőforrás-igényessé válnak. Ez a gyakorlatban a vizsgálatok elhúzódásához és a humán erőforrások túlterheléséhez vezethet.

A téma aktualitását az is erősíti, hogy a nemzetközi és ágazati szakirodalomban egyre hangsúlyosabban jelenik meg a mesterséges intelligencia. Különösen a gépi tanulás és a természetes nyelvfeldolgozás integrálása látható a kiberbiztonsági megfelelésértékelési folyamatokba, a kontrollok folyamatos monitorozásába és az auditbizonyítékok automatizált gyűjtésébe.

A kutatás szempontjából kulcskérdés, hogy a kiberbiztonsági auditok során használt szöveges auditdokumentumok – szabályzatok, tervek, nyilvántartások, jelentések – mennyiben alkalmasak strukturált, algoritmikus feldolgozásra, és hogyan illeszthetők be az MI eszközei a hazai auditmódszertanba. Ennek tisztázása azért különösen fontos, mert egyszerre jelenik meg az az elvárás, hogy az auditfolyamatok megfeleljenek a szigorodó jogszabályi követelményeknek és nemzetközi ajánlásoknak, miközben a szervezetek és az auditorok részéről is erős nyomás van a hatékonyság növelésére és az erőforrásigény csökkentésére.

A témát tovább árnyalja az az ellentmondás, hogy az MI-alapú automatizálás egyfelől jelentősen javíthatja az auditok lefedettségét és gyorsaságát, másfelől új kockázatokat teremt az átláthatóság, az MI-rendszerek saját megfelelősége és felülvizsgálhatósága tekintetében. Ezért a kiberbiztonsági auditok és a mesterséges intelligencia kapcsolatának vizsgálata nemcsak a folyamatok hatékonyságának növelése, hanem a jövőbeni szabályozói elvárások, felelősségi kérdések és a kritikus infrastruktúrák biztonságának szempontjából is kiemelten fontos kutatási terület.

A kutatás hatóköre

A hazai implementáció jelenlegi állapotában az alap biztonsági osztályba sorolt elektronikus információs rendszerekhez rendelt 164 védelmi intézkedés képezi azt a minimális, de minden érintett szervezetnél kötelező kontrollkészletet, amelyre a megfelelésértékelés első hulláma épül. A tanulmány ezért az auditautomatizálási kérdéseket e kontrollkészlethez kapcsolódó auditbizonyítékokra fókuszálva vizsgálja.

A továbbiakban a vizsgálat kizárólag az alap biztonsági osztályhoz rendelt védelmi intézkedésekhez kapcsolódó dokumentumvizsgálat, interjú és tesztelés során keletkező evidenciákat elemzi mint a NIS2-alapú hazai kiberbiztonsági auditmódszertan

[3] NIST 2020.
[4] NIST 2022.

kiindulópontját. Ezzel biztosítható, hogy az MI-alapú automatizálhatósági eredmények közvetlenül értelmezhetők legyenek a gyakorlatban már alkalmazott hazai módszertan szempontjából.

Kutatási kérdés

A jelen kutatás központi kérdése, hogy mely auditbizonyíték-típusok alkalmasak leginkább MI-alapú vizsgálatra és algoritmikus feldolgozásra a NIS2-irányelvnek való megfeleléshez végzett kiberbiztonsági auditok során. A vizsgálat fókusza az SZTFH rendelet[5] szerinti módszertan alapján lefolytatott auditok azon részére esik, amely az alap biztonsági osztályba sorolt elektronikus információs rendszerekhez rendelt 164 védelmi intézkedés teljesülését értékeli. A kutatás azt elemzi, hogy a dokumentumvizsgálat, az interjú és a tesztelés során keletkező különböző formátumú evidenciák miként integrálhatók mesterségesintelligencia-modellekbe.

Célkitűzés

Célul tűztem ki a magyarországi NIS2-alapú kiberbiztonsági auditmódszertan fejlesztési lehetőségeinek feltárását az alap biztonsági osztályba sorolt elektronikus információs rendszerek körében. Célom megállapítani, hogy a kiberbiztonsági auditokban használt dokumentumok és digitális bizonyítékok milyen mértékben alkalmasak strukturált, algoritmikus feldolgozásra. A vizsgálat során rendszerezem az auditokhoz kapcsolódó dokumentumtípusokat és egyéb evidenciákat, illetve saját auditbizonyíték-tipológiát (T1–T7) dolgozok ki. Ennek során a vizsgálati eljárást, a bizonyíték formátumát és az alkalmazható MI-technológiát együttesen veszem figyelembe. A tipológia elkészítése után elemzem, hogy ezek az MI-technológiák miként illeszthetők be a jelenlegi manuális auditgyakorlatba anélkül, hogy sérülne az auditfolyamat bizalmasságára vonatkozó szigorú előírás. Célom javaslatot tenni olyan fejlesztési irányokra, amelyek támogatják a kiberbiztonsági auditok hatékonyságának növelését és a megfelelőség biztosítását.

Módszer

A tanulmány feltáró jellegű kutatás, amelynek célja a hazai NIS2-alapú kiberbiztonsági auditmódszertan és az MI alkalmazási lehetőségei közötti kapcsolódási pontok rendszerezett feltárása. Ennek megfelelően a kutatás módszertani alapját a releváns jogszabályi, nemzetközi ajánlási és tudományos-szakmai források célzott, kvalitatív feldolgozása képezi.

A forrásbázis három pillérre épül. Egyrészt a normatív keretet meghatározó jogforrásokra, különösen a NIS2 irányelvre, a 2024. évi LXIX. törvényre, a 7/2024. (VI. 24.) MK rendeletre és az 1/2025. (I. 31.) SZTFH rendeletre. Másrészt a módszertani háttérre,

[5] 1/2025. (I. 31.) SZTFH rendelet.

elsősorban a NIST SP 800-53 Rev. 5 és a NIST SP 800-53A Rev. 5 dokumentumokra. Harmadrészt pedig azokra a hazai és nemzetközi szakirodalmi forrásokra, amelyek a kiberbiztonsági auditok, a *compliance*-automatizálás, a természetesnyelv-feldolgozás, az OCR, a *computer vision,* az anomáliadetektálás és a magyarázható mesterséges intelligencia alkalmazhatóságát tárgyalják.

A szakirodalom-feldolgozás során a bevont források kiválasztása relevanciaalapon történt. A beválasztás elsődleges szempontja az volt, hogy az adott munka közvetlenül kapcsolódjon legalább egyhez a következő tématerületek közül: kiberbiztonsági audit, megfelelőségértékelés, NIS2- vagy kontrollalapú auditmódszertan, illetve mesterséges intelligencia alkalmazása dokumentum-, log- vagy vizuális bizonyítékok feldolgozásában. A kizárás szempontjai közé tartoztak azok a források, amelyek kizárólag általános MI-alkalmazásokat tárgyaltak audit- vagy megfelelőségi kontextus nélkül, illetve amelyek nem nyújtottak érdemi módszertani vagy technológiai kapcsolódást a vizsgált problémához.

Az elemzés kvalitatív tartalomelemzési logikát követett. A feldolgozott forrásokból először az auditfolyamat szempontjából releváns bizonyítékformátumokat, majd az ezekhez rendelhető technológiai feldolgozási módokat azonosítottam. Ezt követően a hazai auditmódszertanban megjelenő három fő vizsgálati eljárás – dokumentumvizsgálat, interjú, tesztelés – szolgált elsődleges rendezőelvként. A második rendezőelvet a bizonyíték formátuma jelentette, amely alapján a strukturált szöveg, félig strukturált adat, vizuális vagy zárt dokumentum, hangalapú szöveg, jegyzőkönyvi szöveg, valamint log- és eseményadat különült el. A harmadik rendezőelv az elsődlegesen alkalmazható MI-technológia volt, vagyis az, hogy az adott bizonyítéktípus esetében mely technológia jelent reális belépési pontot az automatizált feldolgozáshoz.

E három szempont metszetében jött létre a szerző által kialakított T1–T7 auditbizonyíték-tipológia. A T1–T7 kategóriákhoz az MI-technológiák hozzárendelése funkcionális megfeleltetés alapján történt, vagyis annak figyelembevételével, hogy az adott evidenciatípus elsődlegesen milyen adatformátumban áll rendelkezésre, és e formátum gépi feldolgozására a szakirodalom szerint mely technológia alkalmas.

A módszer eredménye egy fogalmi és módszertani keret, amely megalapozhat későbbi kvantitatív vagy esettanulmány-alapú vizsgálatokat.

Kiberbiztonsági szabályozás Magyarországon

Az európai irányelvek nem alkalmazandók közvetlenül a tagállamokban, így a NIS2 direktíva előírásait a nemzeti jogrendszerekbe kellett integrálni. Magyarország az első tagállamok között volt, amelyek megkezdték a NIS2 irányelv átültetését a hazai jogrendbe. A 2024. évi LXIX. törvény 2025. január 1-jén lépett hatályba. A törvény a Szabályozott Tevékenységek Felügyeleti Hatóságát (SZTFH) jelölte ki általános nemzeti kiberbiztonsági hatóságként, amely felügyeli az érintett szervezetek megfelelőségét és a nyilvántartásba vételi folyamatokat. Mivel a törvény csak a kereteket adja meg, a Miniszterelnöki Kabinetirodát vezető miniszter 7/2024. (VI. 24.) rendelete[6] rögzíti az elektronikus információs rendszerek biztonsági osztályba sorolásának

[6] 7/2024. (VI. 24.) MK rendelet.

követelményeit, valamint az egyes biztonsági osztályokhoz (alap, jelentős, magas) rendelt konkrét védelmi intézkedéseket. Fontos tudományos és szakmai aspektus, hogy ez a rendelet az Egyesült Államok szabványügyi és méréstechnikai hivatalának NIST SP 800-53 Rev. 5 számú, nemzetközileg elismert kontrollkatalógusára épül. Ez az adaptáció biztosítja, hogy a magyar szervezetek a széles körben alkalmazott nemzetközi technológiai és szervezési intézkedéseket alkalmazzák az adatvagyonuk és a rendszereik védelmében.

Míg az MK rendelet az információs rendszerek felett rendelkező szervezetek számára fogalmaz meg védelmi követelményeket, addig az 1/2025. (I. 31.) SZTFH rendelet a megfelelés ellenőrzésének gyakorlati szabályait fekteti le. Ez a jogszabály határozza meg a kiberbiztonsági audit lefolytatásának rendjét, az auditori módszertant és az auditok legmagasabb díját. A rendelet módszertani alapját a NIST SP 800-53A rev5 képezi, amely strukturált eljárásokat biztosít a kontrollok hatékonyságának objektív felméréséhez, biztosítva ezáltal az auditok minőségét és a hatósági elvárások teljesülését. Ez a jogszabályi hierarchia auditálható kiberbiztonsági keretrendszer kialakítására kötelezi a gazdaság és a társadalom működése szempontjából kritikus szervezeteket.

Az elektronikus információs rendszerek biztonsági osztályba sorolása

A NIS2 hazai implementációja során a jogalkotó egyértelművé tette, hogy a kiberbiztonság nem kezelhető egyetlen, mindenre egyformán érvényes sablonként. Ahhoz, hogy a védelem ott legyen a legerősebb, ahol a legnagyobb veszteség érheti a szervezetet, az elektronikus információs rendszereket (EIR) saját jelentőségük és kockázati szintjük alapján három osztályba (alap, jelentős, magas) sorolják, amelyek meghatározzák a vizsgálandó kontrollok számát is. A biztonsági osztályba sorolás közvetlenül meghatározza, hogy a szervezetnek a 7/2024 MK rendelet 2. mellékletében, a védelmi intézkedések katalógusában szereplő kontrollok közül mennyit és milyen mélységben kell implementálnia. A kötelező védelmi intézkedéseket az 1/2025. SZTFH rendelet 6. melléklete szervezeti (SZ) és elektronikus információs rendszer (EIR) szintre bontja. Alap biztonsági osztály esetében 164 védelmi intézkedésnek kell megfelelni, ami a kötelező minimum. Ezt a 164 kontrollt minden, a jogszabály hatálya alá tartozó szervezetnek implementálnia kell, még a legkisebb kockázatú rendszerek esetében is. A jogszabályi mellékletek szerzői elemzése (saját kigyűjtés) alapján megállapítható, hogy alap biztonsági osztály esetében a 164 védelmi intézkedés közül 82 szervezeti és 82 EIR-szintű. Jelentős biztonsági osztály esetén az alap biztonsági osztály kontrolljai kiegészülnek további 139 EIR-szintű, szigorúbb követelménnyel, míg a legkritikusabb, magas biztonsági osztályú rendszereknek további 83, gyakran automatizációt, redundanciát és folyamatos valós idejű monitorozást megkövetelő intézkedésnek kell megfelelniük.

Tekintettel a jelen kutatás fókuszára és a szerző gyakorlati tapasztalataira, e tanulmány a továbbiakban kizárólag az alap biztonsági osztályba sorolt elektronikus információs rendszerekkel és az azokra vonatkozó 164 védelmi intézkedéssel – mint a NIS2-alapú hazai kiberbiztonsági auditmódszertan kiindulópontjával – foglalkozik.

Az alaposztályú intézkedések elsősorban az alapvető kiberhigiénia megteremtésére, az erős dokumentációs, szabályozási alapokra és a transzparens folyamatok kialakítására fókuszálnak.[7]

Vizsgálati eljárások

Az audit célja annak objektív, bizonyítékokkal történő alátámasztása, hogy az elvárt védelmi intézkedések megvalósítása hiánytalan-e, és a gyakorlatban a tervezett módon működnek-e. A vizsgálat során az auditor három fő módszert alkalmaz: dokumentumvizsgálatot, interjút és tesztelést.

Dokumentumvizsgálat

A dokumentumvizsgálat a módszertan alapján minden követelménycsoport esetében kötelezően alkalmazandó módszer. A vizsgálódás során az auditornak a 7/2024. MK rendelet alapján többféle dokumentumtípust kell részletesen áttekintenie. Magas szintű irányítási dokumentumok közé tartozik az 1. kontrollcsaládba tartozó információbiztonsági szabályzat, majd minden további kontrollcsalád esetében a szabályzat és az eljárásrend, összesen 18-18 dokumentum.

1. táblázat: Elkészítendő és vizsgálandó dokumentumok

Ssz.	Dokumentum neve	Dokumentum típusa
1.	Kockázatmenedzsment-stratégia	stratégia
2.	Ellátási lánc kockázatmenedzsmentjének stratégiája	stratégia
3.	Folyamatos felügyeleti stratégia	stratégia
4.	Elektronikus információs rendszerek nyilvántartása	nyilvántartás
5.	Karbantartási nyilvántartás	nyilvántartás
6.	Fizikai belépést ellenőrző eszközök nyilvántartása	nyilvántartás
7.	Látogatói belépések nyilvántartása	nyilvántartás
8.	Be- és kiszállításról szóló nyilvántartás	nyilvántartás
9.	Rendszerelemleltár	leltár
10.	Belépésre jogosult személyek listája	lista
11.	Intézkedési terv és mérföldkövei	terv
12.	Kritikus infrastruktúra és kulcsfontosságú erőforrások biztonsági terve	terv
13.	Rendszerbiztonsági terv	terv
14.	Biztonságértékelési terv	terv
15.	Üzletmenet-folytonossági terv	terv
16.	Biztonsági eseménykezelési terv	terv
17.	Beruházási terv	terv
18.	Munkaköri leírások	leírás

Forrás: a szerző szerkesztése

[7] Váczi–Orbók 2025.

További dokumentumfajtaként megjelennek még stratégiák, nyilvántartások, leltárak, listák, tervek, leírások (1. táblázat). Az auditor nem csupán a dokumentumok meglétét ellenőrzi, hanem azt is vizsgálja, hogy a szabályzatok naprakészek-e, amennyiben szükséges, akkor a megfelelő személy által jóváhagyottak-e, és hogy összhangban állnak-e a jogszabályi előírásokkal és a valós szervezeti környezettel, tehát tartalmilag minimálisan a jogszabály által elvártaknak megfelelnek-e.

Interjú

Az interjú célja, hogy az auditor személyes interakciókon keresztül gyűjtsön további bizonyítékokat, tisztázza a felmerült kérdéseket, és megismerje a leírt folyamatok, eljárások tényleges, gyakorlati megvalósulását. A szóban megbeszélteket ezután alátámasztó dokumentumokkal, evidenciákkal igazolja a szervezet, amiket megküld az auditornak, aki ezekre hivatkozva bővíti az adott kontrollról írt értékelő leírását.

Tesztelés

A tesztelés az audit leggyakorlatiasabb része, ahol az auditor a tényleges és az elvárt működés összehasonlítása érdekében megvizsgálja a rendszerek működését. Ezen a ponton kell a szervezetnek azokat a konkrét evidenciákat (bizonyítékokat) bemutatnia, amelyek technológiailag is igazolják a megfelelést, például határvédelmi megoldások konfigurációjáról vagy jelszókomplexitási beállításokról készült képernyőképekkel, szervezeti tevékenységek és rendszeresemények naplóival. A tesztelési bizonyítékok jelentős része nem tisztán szöveges, gépileg könnyen olvasható formátumú. A technológiai kontrollok beállításait és működését leggyakrabban a rendszerekből kimentett képernyőképekkel, jellemzően PNG, JPG és hasonló képformátumokkal támasztják alá.

Új technológiák a kiberbiztonsági auditokban

Az információbiztonsági auditorokkal szemben szigorú követelmények vannak.[8] A hagyományos, tisztán manuális vizsgálatok rendkívül idő- és erőforrás-igényesek. Ezen komplexitási és kapacitásproblémák kezelésére a szakirodalom egyre hangsúlyosabban az MI-technológiák integrációját javasolja. Fehér elméleti alapvetése szerint[9] az MI képes érdemben növelni a védelmi intézkedések ellenőrzésének hatékonyságát, az ismétlődő folyamatok automatizálását. Ezt az irányvonalat támasztják alá Folorunso és munkatársai,[10] akik a kutatásaik alapján megerősítik, hogy az MI az anomáliadetektálás, a csalásfelismerés és a szabályozói jelentések automatizálása révén növeli a hatékonyságot és csökkenti az adminisztratív terheket. A dokumentumalapú

[8] Krasznay 2020; Baglyos 2022; Barna–Kollár–Oroszi 2023.
[9] Fehér 2022.
[10] Folorunso et al. 2024: 167–184.

megfelelésértékelés automatizálásában különösen a természetesnyelv-feldolgozás (*natural language processing,* NLP) játszik jelentős szerepet.[11] Az NLP-modellek képesek a terjedelmes biztonsági szabályzatok, rendszerbiztonsági tervek és egyéb dokumentumok algoritmikus elemzésére, felismerve az ismétlődő mintázatokat, a szabályozási hiányosságokat, az egymásra hivatkozó szabályzatokat vagy a folyamatleírások közötti ellentmondásokat. Ez a folyamat a megfelelésértékelés leginkább időigényes része. Kutatások igazolják, hogy a megfelelően betanított NLP-rendszerek hatékonyságuk által jelentősen csökkenthetik a dokumentumok értelmezésére fordított időt. A pénzügyi szektorban végzett esettanulmányok is jelentős mértékű auditidő-csökkenést és működési költségmegtakarítást mutattak ki a manuális auditfolyamatokhoz képest.[12]

Az auditbizonyítékok nem kizárólag gépileg olvasható, strukturált szövegek formájában állnak rendelkezésre. A megfelelőséget igazoló alapvető irányítási dokumentumokat, mint amilyen az IBSZ, a rendszerbiztonsági terv vagy a kockázatokat felvállaló dokumentáció, a szervezet vezetőjének vagy a kijelölt felelős személynek formálisan jóvá kell hagynia. A technológiai tesztelések és a formálisan jóváhagyott dokumentációk által az auditbizonyítékok egy része vizuális, képi formátumban, például képernyőképek vagy szkennelt, zárt PDF-ek formájában áll rendelkezésre. Ezen gépileg nem olvasható, nem strukturált adatok algoritmikus feldolgozásához az NLP mellett az optikai karakterfelismerő (*optical character recognition,* OCR) és a számítógépes látás *(computer vision)* technológiák integrációja elengedhetetlen.

Az MI auditokba történő beemelése ugyanakkor új etikai, adatvédelmi és átláthatósági kockázatokat is generál, amelyeket a jogi keretrendszereknek szigorúan egyensúlyban kell tartaniuk az információbiztonsági célokkal.[13] A generatív MI-modellek auditcélú alkalmazásának egyik legnagyobb technológiai kockázata a hallucináció. Előfordulhat, hogy az algoritmus a valóságban nem létező kontrollokra (például egy fiktív elemre) hivatkozik, vagy tévesen határozza meg egy adott biztonsági osztály alapkövetelményeit, ami téves megfelelőségi megállapításokhoz vezethet.[14] Ezen kockázatok miatt a szakirodalom és a szabályozói gyakorlat is egybehangzóan az emberi felügyelet *(human-in-the-loop)* kötelező fenntartását és a gépi döntéshozatal teljes visszakövethetőségének *(traceability)* kialakítását szorgalmazza. A legkorszerűbb és legelterjedtebb neurális hálózatok, valamint a mélytanulási *(deep learning)* modellek – bár kiemelkedő alkalmazkodóképességet mutatnak a hálózati anomáliák felismerésében – úgynevezett „fekete doboz" *(black box)* jellegükből fakadóan alapvetően alkalmatlanok az átlátható és megismételhető logikai láncok biztosítására.[15] Ezekből a gépi tanulási algoritmusokból hiányzik az egzakt szabály-visszavezetés képessége. Döntéseiket átláthatatlan matematikai súlyozásokra és statisztikai korrelációkra alapozzák, nem pedig olyan transzparens, következtethető logikára, amely egy audit során elvárás lenne. Mivel a rendszerek nem képesek megindokolni egy-egy hiányosság okát, kimeneteik önmagukban, emberi felülvizsgálat nélkül nem szolgáltatnak

[11] Smith 2024.
[12] Smith 2024.
[13] Folorunso et al. 2024.
[14] Váczi–Orbók 2025.
[15] Loumachi et al. 2025.

jogilag és szakmailag elfogadható auditbizonyítékot. Ez az átláthatatlanság jelentősen hátráltatja a technológiába vetett felhasználói és szabályozói bizalom kialakulását.[16]

Ezzel a megközelítéssel szemben a szimbolikus MI-modellek architektúrájukból fakadóan más tulajdonságokkal bírnak. Mivel előre definiált, világos szabálykészletek mentén működnek, natív módon garantálják a magyarázhatóságot. A szakirodalom e technológiai dilemma feloldását elsődlegesen a magyarázható mesterséges intelligencia (*explainable AI,* XAI) eszközök integrációjában látja.[17] Az XAI-technológiák célja, hogy láthatóvá váljanak az MI döntéshozatali folyamatai, lehetővé téve, hogy az algoritmus megmutassa a munkáját, azaz világos, transzparens és auditálható nyomot biztosítson az összegyűjtött bizonyítékokról.[18] Az átláthatóság megteremtése nemcsak a bizalmat növeli, hanem kritikus feltétele annak, hogy az auditor megérthesse az automatizált megfelelőségi vizsgálatok eredményeit.

A nemzetközi szakirodalom az MI-alapú kiberbiztonsági auditokat a folyamatos ellenőrzés megteremtésének eszközeként is leírja. Ennek oka a technológiai környezet olyan mértékű előrehaladása, amely a sebezhetőségvizsgálat és a megfelelőségértékelés hatékonyságát növeli.[19] Anwar bemutatja, hogy a gépi tanulásra épülő algoritmusok – a korábban azonosított sérülékenységek mintázataira támaszkodó, felügyelt tanulási modellek, valamint a címkézetlen adatokból rendellenes viselkedést feltáró nem felügyelt tanulási eljárások – képesek gyorsítani a sebezhetőségazonosítást, csökkenteni az emberi hiba kockázatát és proaktívabbá tenni az auditfolyamatot. A természetesnyelv-feldolgozásra épülő eszközök emellett támogathatják a szabályozói követelmények, például adatvédelmi és pénzügyi megfelelőségi keretek szöveges előírásainak automatikus feldolgozását, a belső szabályzatokkal való összevetését és a hiányosságok gyors jelzését.[20]

Aliliele és munkatársai áttekintése az MI-vel támogatott folyamatos auditálási rendszerekre fókuszál, amelyek a hagyományos, időszakos vizsgálatokkal szemben folyamatos adatgyűjtésre és közel valós idejű elemzésre épülnek. A tanulmány szerint a gépi tanulás, a természetesnyelv-feldolgozás és az anomáliadetektálás együttes alkalmazása lehetővé teszi a hozzáférés-ellenőrzés, a konfigurációmenedzsment, az incidenskezelés és a szabályozói megfelelőség folyamatos monitorozását. Ezzel együtt a riasztáskezelés és az automatizált jelentéskészítés csökkenti az audit operatív terheit. A szerzők ugyanakkor rámutatnak arra, hogy az ilyen rendszerek sikeres bevezetése feltételezi az adatok minőségét biztosító vezetői kereteket, a magyarázható mesterséges intelligencia elveinek érvényesítését, valamint azt, hogy az auditorok szerepe a manuális ellenőrzésből a gépi eredmények értelmezésére és felügyeletére épülő szakértői kontroll irányába mozdul el.[21]

A mesterséges intelligencia kiberbiztonsági auditokban betöltött szerepe tehát kettős: egyszerre kínál jelentős hatékonyságnövelést, és hoz magával új, kezelendő kockázatokat. A nemzetközi áttekintés rámutat arra, hogy a gépi tanulás

[16] Loumachi et al. 2025.
[17] Folorunso et al. 2024; Smith 2024.
[18] Kewat 2025.
[19] Anwar 2023.
[20] Anwar 2023.
[21] Aliliele 2025.

és a természetesnyelv-feldolgozás különösen a nagy mennyiségű, szabályozási tartalmú dokumentumok elemzésében, a sebezhetőségek azonosításában és az anomáliák feltárásában kínál érdemi automatizálási potenciált. Ez mérhető auditidő-csökkenést és erőforrás-megtakarítást eredményezhet. Ugyanakkor hangsúlyos, hogy az auditbizonyítékok egy része vizuális vagy zárt formátumú, ezért – mint említettük – az optikai karakterfelismerés és a számítógépes látás bevonása nélkül nem alakítható át megbízhatóan gépileg értelmezhető adattá. Az MI-vel támogatott auditálás felé mutató nemzetközi trendek ugyanakkor egyértelművé teszik azt is, hogy az automatizált elemzés és az emberi szakértői kontroll elválaszthatatlanul egymásra épül.

Auditbizonyíték-tipológia

Az auditbizonyíték-tipológia T1–T7 kategóriák kialakítása a hazai auditmódszertan három fő vizsgálati eljárásának és az ezek során tipikusan előforduló bizonyítékformátumoknak az összevetéséből jött létre. A kategorizálás első szintjén az SZTFH-módszertan szerinti dokumentumvizsgálat, interjú és tesztelés szolgált rendezőelvként. A második szinten a bizonyíték formátuma alapján különülnek el a strukturált szövegek (például információbiztonsági szabályzatok, rendszerbiztonsági tervek), a félig strukturált adatok (leltárak, jogosultsági táblázatok, űrlapok), a strukturálatlan szöveges anyagok (interjújegyzőkönyvek, szabad szövegű jelentések), valamint a vizuális bizonyítékok (képernyőképek, beszkennelt, zárt PDF-ek). Az MI-technológiai dimenzió ezzel párhuzamosan azokat a fő eszközcsoportokat jelöli, amelyek a különböző formátumú bizonyítékok algoritmikus elemzését lehetővé teszik, vagyis a már említett természetesnyelv-feldolgozást (NLP), az optikai karakterfelismerést (OCR), illetve a gépi tanuláson alapuló log- és mintázatelemzést, ideértve a számítógépes látás *(computer vision)* megoldásait is. A végleges T1–T7 felosztás célja az volt, hogy a hazai auditgyakorlatban ténylegesen előforduló bizonyítéktípusok mindegyike egyértelműen besorolható legyen, és egyben összekapcsolhatóvá váljon az elsődlegesen releváns MI-technológiával.

Az auditbizonyítékok MI-szempontú értelmezése

A saját auditbizonyíték-tipológia nemcsak leíró kategóriákat ad, hanem lehetővé teszi az egyes bizonyítéktípusok MI-szempontú minősítését is. A 2. táblázat tartalmazza, hogy mely bizonyítékformátumok esetében reális a mesterséges intelligencia részleges vagy akár jelentős mértékű bevonása. A táblázat a T1–T7 típusok mellett röviden összefoglalja az adott bizonyítékra jellemző automatizálhatósági lehetőségeket, így kirajzolva, hogy a magyar NIS2-alapú auditgyakorlatban mely területek kínálják a legkézenfekvőbb MI-fejlesztési célpontokat. A hozzárendelés minden esetben abból indult ki, hogy az adott bizonyítéktípus milyen módon tehető gépileg értelmezhetővé és auditcélból feldolgozhatóvá.

2. táblázat: Auditbizonyíték-típusok MI-szempontú elemzése

Kód	Vizsgálat típusa	Bizonyíték formátuma	Példa	Javasolt MI-technológia
T1	Dokumentumvizsgálat	Strukturált szöveg	Információbiztonsági szabályzat, rendszerbiztonsági terv, eljárásrendek	NLP (szövegértelmezés, kulcsszavas és szemantikus keresés)
T2	Dokumentumvizsgálat	Félig strukturált szöveg (táblázat, jegyzék)	Eszközleltár, jogosultsági mátrix, incidens-nyilvántartás	NLP + klasszikus ML (mezőkivonás, konzisztencia-ellenőrzés)
T3	Dokumentumvizsgálat	Vizuális/zárt dokumentum (szkennelt, aláírt irat)	Beszkennelt IBSZ, formálisan jóváhagyott nyilatkozatok, zárt PDF-ek	OCR + NLP (karakterfelismerés, tartalmi ellenőrzés)
T4	Interjú	Hangfelvételből szöveg	Felelősökkel készített strukturált interjúk, *kick off* megbeszélés rögzítése	ASR + NLP (átiratkészítés, kulcstémák és hiányzó elemek azonosítása)
T5	Interjú	Szöveges jegyzőkönyv, emlékeztető	Interjújegyzőkönyvek, összefoglalók, emlékeztetők	NLP (kivonatolás, ellentmondás-keresés, szabályzatokkal való összevetés)
T6	Tesztelés	Logfájlok, eseményadatok (strukturált vagy félig strukturált)	Hozzáférési naplók, hálózati forgalmi logok, tűzfallogok	ML/anomáliadetektálás (felügyelt és nem felügyelt tanulás)
T7	Tesztelés	Vizuális bizonyíték (képernyőkép, UI-kimenet)	Konfigurációs képernyőképek (PNG, JPG), biztonsági beállítások grafikus felületről mentett képei	Computer vision + OCR (UI-elem felismerése, beállítások kinyerése)

Forrás: a szerző szerkesztése

A dokumentumvizsgálat során használt strukturált szöveges bizonyítékok (T1) esetében a természetesnyelv-feldolgozás alkalmazása különösen ígéretes, mivel a szabályzatok és tervek sablonszerű felépítése, ismétlődő szóhasználata és jól definiált jogszabályi háttérre való hivatkozása támogatja a kulcsfogalmak automatikus keresését, a követelményekhez rendelést és a hiányosságok jelzését. A félig strukturált dokumentumok (T2) már egyrészt táblázatos jellegük, másrészt a mezők közötti kapcsolatok miatt igénylik a szöveges modelleket kiegészítő, klasszikus gépi tanulási módszerek bevonását.

A vizuális vagy zárt formátumú dokumentumok (T3) és a tesztelési bizonyítékok körébe tartozó képernyőképek (T7) esetében a gépi feldolgozás első lépését az optikai karakterfelismerés jelenti, amely a képi formátumú tartalmat gépileg olvasható szöveggé alakítja. Ezt követően a szöveg már NLP-vel, a képi elemek pedig számítógépes látási algoritmusokkal elemezhetők. Ugyanakkor a tipológia már ebben a pontban rámutat arra, hogy ezeknél a bizonyítéktípusoknál a feldolgozás pontossága függ az elrendezéstől és a vizuális zajtól, emiatt – mint korábban erre felhívtuk a figyelmet – a teljes automatizálás csak erős humán ellenőrzés mellett képzelhető el.

Az interjúalapú bizonyítékoknál a tipológia külön kategóriába sorolja a hangfelvételről automatikusan készített átiratokat (T4) és a közvetlen szöveges jegyzőkönyveket (T5). Előbbi esetben az automatikus beszédfelismerés (ASR) és az NLP együttes

alkalmazása teszi lehetővé a kulcstémák, hiányzó elemek és esetleges ellentmondások azonosítását, míg a jegyzőkönyvek közvetlenül alkalmasak kivonatolásra és a formális szabályzatokkal, eljárásrendekkel való összevetésre. A tesztelési eljárások során keletkező fájlok és eseményadatok (T6) a gépi tanulás szempontjából önálló, kiemelt kategóriát alkotnak: folyamatos monitorozásra, trend- és anomáliadetektálásra használhatók, és lehetőséget teremtenek arra, hogy az auditor ne csupán pillanatfelvételek alapján ítélje meg a kontrollok működését. Ez előrevetíti az auditmódszertan fejlődése mellett az auditra való felkészülés módját is, valamint az egész audit folyamatának átalakíthatóságát.

Következtetés

A tanulmány újszerűsége abban áll, hogy a magyar NIS2-alapú kiberbiztonsági auditmódszertan alap biztonsági osztályú védelmi intézkedéseihez kapcsolódó auditbizonyítékokat MI-szempontú tipológiai keretbe rendezi. Emellett a különböző evidenciákhoz konkrét, technológiailag releváns MI-eszközcsoportokat rendel. A tanulmány rámutat, hogy a hazai NIS2-alapú kiberbiztonsági auditmódszertan ugyan strukturált, jogszabályokra és nemzetközi ajánlásokra épülő keretet biztosít, a gyakorlatban használt auditbizonyítékok jelentős része mégis nehezen vagy egyáltalán nem gépileg olvasható formátumban áll rendelkezésre. A saját auditbizonyíték-tipológia megmutatta, hogy a dokumentumvizsgálat, az interjú és a tesztelés során keletkező bizonyítékok formátum és tartalom szerint jól elkülöníthető csoportokba rendezhetők, és ezekhez egyértelműen hozzárendelhetők a releváns MI-technikák. A gyakorlati következmények szempontjából ez azt jelenti, hogy rövid távon érdemes az MI-fejlesztéseket elsősorban a szabályzatok, tervek, eljárásrendek algoritmikus elemzésére fókuszálni, mivel ez a terület úgy kínál érdemi hatékonyságnövekedést, hogy közben a módszertani és megfelelőségi kockázatok kezelhetők maradnak. A vizuális bizonyítékok esetében jelenleg elsősorban az OCR és a számítógépes látás előfeldolgozó szerepe indokolt, miközben a végső értékelői döntés felelőssége továbbra is az auditoroknál marad.

A tipológia egyúttal alapot teremt egy későbbi, kvantitatív jellegű vizsgálat számára is, amelyben az egyes bizonyítéktípusok MI-alapú automatizálhatósága és kockázati szintje – például külön automatizálhatósági és kockázati mutatók formájában – számszerűen értékelhető. Jelen tanulmány ezért elsősorban a fogalmi keretek megteremtésére és a legfontosabb technológiai paraméterek azonosítására koncentrál.

Felhasznált irodalom

Aliliele, Chime et al. (2025): A Review of AI Assisted Continuous Auditing Systems in Technology Risk and Cybersecurity Oversight. *Gyanshauryam, International Scientific Refereed Research Journal,* 8(4), 210–250. Online: https://doi.org/10.32628/GISRRJ258369

Anwar, Mohammed (2023): Elevating Cybersecurity Audits. How AI is Shaping Compliance and Threat Detection. *Aitoz Multidisciplinary Review,* 2(1), 35–43. Online: www.academia.edu/127357785/Elevating_Cybersecurity_Audits_How_AI_is_Shaping_Compliance_and_Threat_Detection

Baglyos Sándor (2022): Az információbiztonsági auditálás fontossága. *Ludovika.hu,* 2022. június 23. Online: www.ludovika.hu/blogok/cyberblog/2022/06/23/az-informaciobiztonsagi-auditalas-fontossaga

Barna Bianka Rita – Kollár Csaba – Oroszi Eszter Diána (2023): A social engineering helye az információbiztonsági auditban. *Biztonságtudományi Szemle,* 23(1), 25–41. Online: https://real-j.mtak.hu/26698/1/Biztons%C3%A1gtudom%C3%A1nyi_Szemle_2023_5_1.pdf

Fehér András Tibor (2022): Mesterséges intelligencia a kibervédelemben. In Szelei Ildikó (szerk.): *A hadtudomány aktuális kérdései napjainkban II.* Budapest: Ludovika Egyetemi Kiadó, 123–137. Online: https://openaccess.ludovika.hu/nke/catalog/download/185/1520/3619?inline=1

Folorunso, Adebola et al. (2024): Impact of AI on Cybersecurity and Security Compliance. *Global Journal of Engineering and Technology Advances,* 21(1), 167–184. Online: https://doi.org/10.30574/gjeta.2024.21.1.0193

Kewat, Rajnish (2025): Why Is the Use of AI in Cybersecurity Audits Rising Among Regulated Industries? *Cyber Security Training Institute,* 2025. augusztus 2. Online: www.cybersecurityinstitute.in/blog/why-is-the-use-of-ai-in-cybersecurity-audits-rising-among-regulated-industries

Krasznay Csaba [@The Prof and The Geek] (2020): Információbiztonsági audit. *YouTube,* 2020. április 2. Online: www.youtube.com/watch?v=nb0GQQyCG6I

Loumachi, Fatma Yasmine et al. (2025): AI in Control. Rethinking Cybersecurity Compliance and Auditing. *Information and Software Technology,* 195. Online: https://doi.org/10.1016/j.infsof.2026.108132

NIST (2022): *Security and Privacy Controls for Information Systems and Organizations.* NIST Special Publication 800-53, Revision 5. Gaithersburg: National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.SP.800-53r5

NIST (2020): *Assessing Security and Privacy Controls in Information Systems and Organizations.* NIST Special Publication 800-53A, Revision 5. Gaithersburg: National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.SP.800-53Ar5

Smith, Jane (2024): The Role of Natural Language Processing in Automating Cybersecurity Compliance Audits. *Distributed Learning and Broad Applications in Scientific Research,* 24(10), 360–366. Online: https://dlabi.org/index.php/journal/article/view/163

Váczi Dániel – Orbók Ákos szerk. (2025): *Whitepaper: NIS 2 Magyarországon.* Budapest: Dr. Váczi Dániel. Online: www.nis2whitepaper.eu/hu/_files/ugd/3dac62_3efe3e64753d4d0faa561b6cd69cd880.pdf

Jogi források

2024. évi LXIX. törvény Magyarország kiberbiztonságáról. Online: https://njt.hu/jogszabaly/2024-69-00-00

7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről. Online: https://njt.hu/jogszabaly/2024-7-20-7G

1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról. Online: https://njt.hu/jogszabaly/2025-1-20-8K

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:L_202590613