A Mesterséges Intelligencia (MI) rendszerek besorolása az EIR struktúrába

VFP2 KiberVéd - NIS2 Audit felkészítés szakmai iránymutatás 2026/9

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.02.20	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

A Szabályozott Tevékenységek Felügyeleti Hatósága által véleményezett dokumentum

1 VEZETŐI ÖSSZEFOGLALÓ

Jelen állásfoglalás célja, hogy a mesterséges intelligencia rendszereket a Kiberbiztonsági tv. szerinti elektronikus információs rendszer (EIR) struktúrába illessze, és egyértelmű besorolási szempontokat adjon NIS2 felkészüléshez.

A besorolás központi elve, hogy nem a „MI" technológiai címke számít, hanem az adat útja, a feldolgozás helye és a szervezet rendelkezési joga az erőforrás felett. Ennek megfelelően SaaS/felhős MI-szolgáltatások és az API-alapú integrációk a felhős szolgáltatások közé kerülnek, ahol az adatok elhagyják a szervezetet, a kontroll főként hozzáférés-kezelésre, konfigurációra és adatküldési szabályokra terjed ki.

Az on-premise, saját üzemeltetésű MI egyértelműen saját EIR-nek minősül, ahol a szervezet teljes körű rendelkezési joggal és felelősséggel bír az infrastruktúra, a modell és az adatok felett, így az auditmélység is a legnagyobb. A shadow MI (magánfiókok, árnyékinformatika) nem tekinthető EIR-nek, ugyanakkor kiemelt biztonsági kockázat, amelyet szabályzással, oktatással és technikai kontrollokkal kell kezelni. Minden MI-használatot szerepeltetni kell az EIR-nyilvántartásban, mert az „elfelejtett" MI-rendszerek megnövelik az adatszivárgás és megfelelési kockázatot.

2 A VIZSGÁLANDÓ KÉRDÉS

Hogyan soroljuk be Mesterséges Intelligencia (MI) rendszereket az EIR struktúrába?

3 VÁLASZ

3.1 Fogalmi behatárolás

3.1.1 MI rendszer

A magyar jogrendszerben a mesterséges intelligencia rendszerek fogalmát közvetlenül a mesterséges intelligenciáról szóló uniós rendelet (AI Act)[1] határozza meg. A hazai végrehajtási törvény rögzíti, hogy a fogalmakat az uniós rendelet szerint kell értelmezni.

> *„Ha e törvény eltérően nem rendelkezik, az e törvényben és az annak végrehajtását szolgáló jogszabályokban alkalmazott fogalmakat az (EU) 2024/1689 európai parlamenti és tanácsi rendelet 3. cikkében szereplő*

[1] Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet).

meghatározások szerinti tartalommal kell értelmezni." [2025. évi LXXV. törvény 2. §]

Ennek megfelelően az MI rendszer pontos jogi definíciója a következő:

„»MI-rendszer«: gépi alapú rendszer, amelyet különböző autonómiaszinteken történő működésre terveztek, és amely a bevezetését követően alkalmazkodóképességet tanúsíthat, és amely a kapott bemenetből explicit vagy implicit célok érdekében kikövetkezteti, miként generáljon olyan kimeneteket, mint például előrejelzéseket, tartalmakat, ajánlásokat vagy döntéseket, amelyek befolyásolhatják a fizikai vagy a virtuális környezetet;" [AI Act 3. cikk 1. pont]

A definíció kulcselemei a következők:

- a rendszer gépi alapú, tehát szoftveres vagy hardveres környezetben fut;
- képes bizonyos fokú autonómiára, vagyis emberi beavatkozás nélkül is képes részfeladatok végrehajtására;
- alkalmazkodóképességgel rendelkezhet, azaz képes lehet a működése során tanulni vagy változni;
- következtetési képességgel bír, amellyel a bemeneti adatokból kimeneteket (tartalmat, döntést, előrejelzést) generál.

Fontos tisztázni, hogy az AI Act nem tartalmaz önálló definíciót a „generatív MI" (generative AI) kifejezésre a 3. cikk fogalommeghatározásai között. Ehelyett a jogalkotó az „általános célú MI-modell" kategóriáját használja a szabályozás alapjaként, amely magában foglalja a generatív modelleket is.

A jogszabály preambuluma azonban kifejezetten összeköti a két fogalmat, és tisztázza a generatív MI helyét a rendszerben.

„A nagy generatív MI-modellek az általános célú MI-modellek tipikus példái, mivel rugalmas tartalomelőállítást tesznek lehetővé, például szöveg, audio, képek vagy videó formájában, amelyekbe könnyen beleillik különféle feladatok széles köre." [AI Act (99) preambulumbekezdés]

A jogi relevanciával bíró definíció tehát az általános célú MI-modell, amelyre a szigorúbb szabályok (pl. átláthatóság, szerzői jogi megfelelés) vonatkoznak:

„»általános célú MI-modell«: olyan MI-modell – ideértve azt is, amikor az ilyen MI-modell tanítása nagy adatmennyiséggel, nagy léptékű önfelügyelet mellett történik –, amely jelentős általánosságot mutat, és forgalomba hozatalának módjától függetlenül, különféle feladatok széles körének elvégzésére képes, valamint többféle downstream rendszerbe

> *vagy alkalmazásba integrálható, azon MI-modellek kivételével, amelyeket a forgalomba hozatalukat megelőzően kutatási, fejlesztési vagy prototípus-alkotási tevékenységekre használnak;" [AI Act 3. cikk 63. pont]*

Az AI Act meghatároz átláthatósági kötelezettségeket az olyan rendszerekre, amelyek szintetikus tartalmat hoznak létre (ez a generatív MI elsődleges funkciója).

> *„A szintetikus hang-, kép-, video- vagy szöveges tartalmat létrehozó MI-rendszerek – köztük az általános célú MI-rendszerek – szolgáltatóinak biztosítaniuk kell, hogy az MI-rendszer kimeneteit géppel olvasható formátumban jelöljék meg, és azok mesterségesen létrehozottként vagy manipuláltként észlelhetők legyenek." [AI Act 50. cikk (2) bekezdés]*

A generatív MI jogi szempontból olyan, jellemzően általános célú MI-modellen alapuló rendszer, amely:

- képes új, szintetikus tartalom (szöveg, kép, hang, videó) létrehozására;
- sokféle feladat elvégzésére alkalmas és különböző alkalmazásokba integrálható;
- specifikus átláthatósági követelmények alá esik, különösen a kimenetek jelölése tekintetében.

3.1.2 Az EIR fogalma

Az elektronikus információs rendszer fogalmát a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.) az alábbiak szerint definiálja:

> *„24. elektronikus információs rendszer: a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési hálózat, b) bármely eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján az adatok automatizált kezelését végzi, ideértve a kiber-fizikai rendszereket, vagy c) a b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;" [2024. évi LXIX. törvény 4. § 24. pont]*

Amennyiben az MI rendszerrel adatokat kezelnek, tárolnak vagy dolgoznak fel, az MI rendszer működtetéséhez használt eszköz vagy eszközök csoportja az a fenti definíció alapján EIR-nek vagy annak elemének minősül.

3.2 Az MI rendszerek besorolása az EIR struktúrába

A kiberbiztonsági audit egyik legkritikusabb lépése az EIR-ek (Elektronikus Információs Rendszerek) helyes azonosítása és besorolása. Az MI rendszerek megjelenése új kihívást jelent, mivel ezek egyszerre viselkedhetnek szoftverként, szolgáltatásként vagy akár adatfeldolgozó platformként. A besorolás kulcsa nem a technológia neve (pl. "MI"), hanem a felhasználás módja, az adatáramlás iránya és a szervezet rendelkezési joga felette.

A besorolást az alábbi kategóriák szerint javasoljuk. Az EIR besorolásnál nem a technológiai "hype"-ra kell a hangsúlyt fektetni, hanem az adat útjára. Ha az adat elhagyja a szervezetet, a rendszert felhő alapon működő szolgáltatóként kell kezelni. Ha az adat nem hagyja el a szervezetet, saját rendszerként kezelendő. Fontos szempont, hogy az MI rendszerek nem hagyhatók ki a leltárból, mert egy "elfelejtett" MI-használat könnyen vezethet adatszivárgáshoz.

3.2.1 SaaS / felhős MI szolgáltatások (publikus modellek előfizetéssel)

Ez a leggyakoribb vállalati felhasználási mód (pl. Anthropic Claude, Grok, ChatGPT, Google Gemini, Microsoft Copilot).

Ezeket a rendszereket célszerű a felhő alapú szolgáltatások közé sorolni, hasonlóan egy Microsoft 365 vagy egy Google Workspace előfizetéshez.

Audit és adatvédelmi szempontból a mechanizmus azonos más felhőszolgáltatásokkal. Az adatok elhagyják a szervezet felügyeleti körét (kikerülnek a felhőbe), majd az eredmény visszatér a szervezet rendszereibe. Az, hogy a háttérben egy nyelvi modell (LLM) végzi a feldolgozást, az EIR besorolás szempontjából másodlagos; a lényeg az adatfeldolgozás kiszervezett jellege.

Audit szempontból itt a szervezetnek korlátozott a rendelkezési joga (nem fér hozzá a szerverekhez, nem módosíthatja a modell forráskódját), a felelőssége elsősorban a hozzáférés-kezelésre (ki használhatja?), a konfigurációra (pl. history mentése ki/be) és a feltöltött adatok kontrolljára terjed ki.

3.2.2 API alapú integráció (beágyazott MI)

Azok az esetek tartoznak ide, amikor a szervezet nem közvetlenül a webes felületen chatel az MI-vel, hanem egy saját fejlesztésű vagy belső szoftver hívja meg a szolgáltató (pl. Gemini, Grok, OpenAI, Anthropic) API-ját.

Bár technikailag különbözik a webes használattól, az audit logikája szerint ez is a felhő alapú szolgáltatásokhoz vagy a kapcsolódó üzleti alkalmazás (pl CRM rendszer) részeként kezelendő.

Az adatvédelmi és információbiztonsági kockázat azonos a SaaS modellel, az adatok elhagyják a szervezet határát, átmennek egy API csatornán, feldolgozzák őket, majd visszatérnek.

Az audit fókuszában a hitelesítés (API kulcsok védelme), a titkosítás (csatornavédelem) és a naplózás áll. A besorolásnál nem feltétlenül kell külön "MI EIR-t" képezni, hanem a hívást kezdeményező üzleti alkalmazás (pl. egy belső szakrendszer vagy üzleti alkalmazás) részeként, annak "külső függőségeként" jelenik meg.

3.2.3 On-premise (saját üzemeltetésű) MI

Ez a legtisztább, de egyben a legnagyobb üzemeltetési terhet jelentő kategória. Ilyenkor a szervezet letölt egy nyílt forráskódú modellt (pl. LLaMA, Mistral) és saját szerverparkon vagy privát felhőben futtatja.

EIR besorolás szempontjából egyértelműen saját EIR-nek minősül. Kezelhető önálló "MI EIR"-ként, vagy ha szorosan integrálódik egy üzleti folyamatba, akkor az "Üzleti rendszerek" csoportba is tehető.

Mivel a szervezet birtokolja a hardvert (vagy a privát felhős erőforrást), a szoftvert és az adatot is, itt a teljes rendelkezési jog érvényesül.

Audit szempontból a szervezet felel minden szintért, az operációs rendszer frissítésétől (patch management) a modell biztonságáig. Itt a legmagasabb a kockázat a konfigurációs hibákra és a sérülékenységekre (pl. elavult vagy hamisított Python könyvtárak), ezért az auditor ezt a területet fogja a legmélyebben vizsgálni.

3.2.4 Shadow IT - shadow AI (árnyékinformatika) és magánfiókok

Azok az esetek tartoznak a „Shadow AI" fogalomkörébe, amikor a munkavállalók a saját, privát fiókjaikat (pl. ingyenes Deepseek, Gemini, Grok, ChatGPT, DeepL) használják céges feladatokra, a szervezet tudta vagy jóváhagyása nélkül.

Ez nem EIR, hanem biztonsági kockázat/ incidensforrás. Nem lehet auditálni a hagyományos értelemben, mivel a cégnek nincs felette rendelkezési joga.

Mivel nem sorolható be hivatalos EIR-ként, a kezelése a szabályozás (tiltás/tűrés) és az oktatás területére esik. A szervezet belső szabályzásában (információbiztonsági szabályzat vagy MI szabályzat) rendelkezéseket kell hozni a Shadow AI jelentette kockázatok kezelése érdekében. Bizalmas információknak a megfelelő bizalmasságot nem garantáló vállalati licensszel nem rendelkező MI rendszerszerekkel való megosztása (akár felületen, akár API-n keresztül) kifejezetten tilos. A Shadow AI legfeljebb kutatási, informálódási célból engedélyezhető.

Érdemes technikai lépéseket is tenni (pl. webfilter, CASB - Cloud Access Security Broker) a Shadow AI blokkolására vagy monitorozására.

4 FELHASZNÁLT FORRÁSOK

- 2025. évi LXXV. törvény az Európai Unió mesterséges intelligenciáról szóló rendeletének magyarországi végrehajtásáról;
- 344/2025. (X. 31.) Korm. rendelet az Európai Unió mesterséges intelligenciáról szóló rendeletének magyarországi végrehajtásáról szóló 2025. évi LXXV. törvény végrehajtásáról;
- Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (AI Act).
- 2024. évi LXIX. törvény a Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről