DOI: https://doi.org/10.12700/btsz.2026.8.2.157

FIRESAFETY IN DATA CENTRES – CURRENT CHALLENGES

ADATKÖZPONTOK TŰZVÉDELMI KÉRDÉSEI – AKTUÁLIS PROBLÉMÁK

SOMOGYI Tamás[1] – NAGY Rudolf[2]

Abstract

The availability of IT services is getting more and more important in the era of digitalisation, especially in case of essential services. Obviously, IT services are provided by servers concentrating in data centres. Moreover, some of the data centres considered part of the critical infrastructure, therefore their security and fire safety is uttermost. Due to their specialities, data centres require special solutions even in the field of fire safety; however, very few studies focused on this topic. The goal of this study is to describe the specialities of data centres' fire safety and explore recent research results to have a better understanding of this important topic.

Keywords

fire, fire safety, data centre

Absztrakt

Digitalizálódó világunkban az elektronikus szolgáltatások rendelkezésre állásának kérdése egyre nagyobb szerepet kap, különösen a társadalom szempontjából alapvetőnek tekinthető szolgáltatások esetében. Minden IT szolgáltatás mögött szükségszerűen megtalálhatóak az IT eszközök, melyek adatközpontokban koncentrálódnak. Az adatközpontok gyakran kritikus infrastruktúra részét képezik, így biztonságuk kérdésköre kiemelt jelentőségű, mely terület része a tűzvédelem is. Az adatközpontok speciális felépítéséből, berendezéséből és használatából fakadóan a tűzvédelem terén egyedi kérdések is felmerülnek, melyek kutatására és tudományos tárgyalására eddig csekély figyelem irányult. Kutatásunk célja feltárni az adatközpontok tűzvédelmi specialitásait, valamint a nemzetközi szakirodalom kutatási irányaiból és eredményeiből leszűrhető következtetések levonása a téma mélyebb megértése érdekében.

Kulcsszavak

tűz, tűzvédelem, adatközpont

[1] somogyit588@gmail.com | ORCID: 0000-0003-1397-697X | PhD student, Óbuda University Doctoral School of Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] nagy.rudolf@uni-obuda.hu | ORCID: 0000-0001-5108-9728 | habil. associate professor, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary | habil. docens, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

Az elmúlt három évtizedben látható digitalizáció jelentősen gyorsítja a gazdaság szerkezetének átalakulását, továbbá országonként és fejlettségi szintenként eltérő módon ugyan, de pozitív hatással bír a termelékenységre [1]. Ez a digitalizáció és IT szolgáltatások vezette fejlődés az utóbbi években gyorsulni látszik az egész világon, így Közép-Európában is [2]. Az ipari tevékenység digitalizációjával [3] és a rutinfeladatok tekintetében a robotizációval [4] párhuzamosan átalakulnak a társadalmi szokások és elvárások, gondoljunk csak az internetes vásárlásra [5], és az elektronikus bankolásra [6]. A közigazgatási szervek mind jobban terjedő elektronikus szolgáltatásokat nyújtanak az állampolgároknak [7], az oktatásban teret nyer a digitális oktatás [8]. Mindezek mellett tény, hogy napjainkban egyre szélesebb körűvé válik a mesterséges intelligencia (MI) megjelenése és alkalmazása, ebből fakadóan kutatások sora foglalkozik az MI felhasználási lehetőségeivel [9], [10], [11] valamint a digitalizáció előidézte biztonsági kihívások kérdéskörével [12], [13], [14].

Az üzleti világ és a magánélet szokásait tekintve kijelenthető, hogy azokat napjainkban a digitalizáció és információtechnológia határozza meg, illetve alakítja át. A JP Morgan felmérése szerint 2026-ban a vállalatok többsége mesterséges intelligencia bevezetését tervezi, 62%-uk folyamatautomatizálás, 44%-uk elemzés, 42%-uk pedig piaci előrejelzés területen [15]. A Chase felmérése is ezt erősíti meg, mely eredménye szerint 2025-ben az MI felhasználása felgyorsult, és ez várható 2026-ban is [16]. A Forbes magazin egyik vonatkozó cikke is az MI térnyerését vetíti előre 2026-ra az üzleti életben, mely egyrészről egyes üzleti folyamatok automatizálását, másfelől MI alapú szolgáltatások nyújtását jelenti [17]. A digitalizáció és a technológia, azon belül is az MI növekvő használata szükségszerűen növekvő mértékben igényli ezen szolgáltatások mögötti IT eszközök üzemeltetését és rendelkezésre állását, hiszen ezek kiesése fennakadást idézhet elő az üzletmenetben, a vállalatok napi működésében [18], termeléskieséshez és pénzügyi veszteséghez is vezethet [19].

A 2026. év eleji iparági hírek és események az adatközponti infrastruktúra világából mindezt alátámasztják. A Digital Edge bejelentette, hogy az indonéziai Bekasi-ban 4,5 milliárd USD befektetéssel megépíti Indonézia egyik legnagyobb adatközpontját [20]. Az Oracle 50 milliárd USD -t tervez költeni 2026-ban MI-t támogató infrastruktúrára [21]. 2026. februári európai hír, hogy Franciaországban Bordeaux-ban épül új adatközpont 3,59 milliárd USD költséggel [22]. A Moody's becslése szerint 2026-2030 között a világon legalább 3 trillió USD-t fordítanak adatközponti infrastruktúra projektekre [23].

Az adatközpontok gyors terjedése még jobban előtérbe helyezi a létesítményi biztonság [24] és a kritikus infrastruktúrák védelmének kérdéskörét [25], [26], [27], [28], [29] valamint azon belül a tűzvédelem különböző aspektusait [30], [31], [32], [33]. Minthogy az adatközpontokban üzemelő, elektronikus szolgáltatásokat nyújtó és a digitalizált adatot tároló IT eszközök védelme és rendelkezésre állása kiemelt jelentőségűvé válik, természetes módon jelenik meg a magas szintű tűzvédelem követelménye ezen speciális létesítményekben, illetve merül fel a tűzvédelem fokozásának igénye.

Kutatási célok és módszerek

A kutatás célja iparági hírek és nyilvánosságra került megtörtént esetek, valamint témabeli tudományos publikációk feldolgozásával egyfelől az adatközpontok tűzvédelmi specialitásainak bemutatása, másfelől a védekezés terén az aktuális kutatási irányokból és

eredményekből leszűrhető következtetések levonása a téma mélyebb megértésének érdekében.

A kvalitatív módszerű, az aktuális kutatási irányok és eredmények felderítését célzó szakirodalmi kutatás a nemzetközi tudományos publikációk egyik kiemelt adatbázisának áttekintésével történt az alábbiak szerint.

- adatbázis: www.sciencedirect.com/
- keresés dátuma: 2026. március 20.
- keresési feltételek:
  - Title, abstract, keywords: „data centre fire“ (ugyanaz az eredmény született „data center“ keresőszóval is, tehát a brit és az amerikai angol alapján keresve nincs különbség)
  - típus: „Research articles“
- eredmény: 24 cikk, melyből 7 cikk releváns, a többi nem tűzvédelemhez kapcsolódik (például tűzfal kérdéskörével foglalkozó)

Az iparági hírek forrása a www.datacenterknowledge.com portál volt, kiegészítve nemzetközi gazdasági elemzőcégek jelentéseivel és hírportálokon megjelenő hírekkel.

ADATKÖZPONTI TŰZESETEK

Az iparági történésekről hírt adó Data Center Knowledge portál több tűzesetet is összegyűjtött [34]. Az amerikai Iowa államban a Google egyik legrégebbi és legnagyobb adatközpontjában tört ki tűz 2022-ben elektromos kisülés következtében, mely eredményeként három ember megsérült és IT szolgáltatásokban kiesés volt tapasztalható. 2021-ben Strassbourgban az OVH adatközpont egyik szerverterme égett le, napokra IT szolgáltatás nélkül hagyva a francia felhőszolgáltató kb. 65 ezer ügyfelét. A texasi AT&T telekommunikációs cég adatközpontjában történt 2018-as tűzeset egy elektromos kapcsoló hibájából, 12 órára internet- és telefonelérés nélkül hagyva ügyfeleit.

2024-ben Szingapúrban egy adatközpont Li-ion akkumulátorainál keletkezett tűzzel a katasztrófavédelem több, mint egy napig küzdött, a tűz okozta kiesést az IT szolgáltatásokban pedig több ázsiai nagyvállalat és vásárlói érezték meg, köztük az Alibaba ügyfelei is [35]. Egy dél-koreai kormányzati adatközpontban az egyik Li-ion akkumulátor csere közben felrobbant és gyorsan terjedő tüzet idézett elő [36]. A tűzeset következménye a kormányzati elektronikus szolgáltatásokban történő fennakadás mellett 125,000 köztisztviselő adatának és nyolc év kormányzati munkadokumentumnak az elvesztése.

Fenti néhány esetből látható, hogy még a kiemelt szerepük miatt különösen védettnek gondolt, és általában elzártan üzemeltetett adatközpontokban is előfordulnak tűzesetek, amiből következik az adatközponti tűzvédelem létjogosultsága és fejlesztési lehetőségei kutatásának a jelentősége.

ADATKÖZPONTOK SAJÁTOSSÁGAI A TŰZVÉDELEM SZEMPONTJÁBÓL

Az épületüzemeltetés és vagyonvédelem kérdésköre mellett kiemelt jelentőségű az adatközpontok biztonságának terén a tűzvédelem témája. Általánosságban elmondható, hogy a tűz az emberi életet is veszélyezteti, mely nyilvánvalóan a legsúlyosabb veszteség, ezen felül pedig anyagi kárt is okozhat. Adatközpontok esetében azonban további vesztesé-

gek is előfordulhatnak, hiszen egy tűz következménye lehet informatikai szolgáltatások kiesése, valamint adatvesztés. Ezért a magas szintű tűzvédelem jogos érdeke az üzemeltetőnek, illetve bérlőknek, továbbá jogos elvárása az IT szolgáltatásokat élvezőknek, végső soron az egész társadalomnak. Kiemelt jelentőséggel bír tehát az adatközponti tűzvédelem kérdésköre, melynél elengedhetetlen figyelembe venni az adatközpontok speciális jellegét.

Az adatközpontok specialitásaként kell említeni az egy helyen koncentrálódó IT eszközök magas számát: a szervereket és kommunikációs hálózati elemeket, valamint további eszközöket. Lényeges, hogy az IT eszközök működésük során hőt termelnek, mely hő elvezetése esszenciális, hiszen ezen eszközök a gyártók ajánlását alapul vevő iparági gyakorlat szerint 18 - 20 Celsius fok között üzemeltethetőek optimálisan [37], tehát az élettartamuk és megfelelő működésük érdekében az állandó hőmérséklet biztosítása kulcskérdés. Lényeges továbbá a páratartalom és a levegő pormentessége is. Ebből fakadóan az adatközpontban az épületüzemeltetési rendszer eszközeivel is számolni szükséges. Ezen felül figyelembe kell venni az IT eszközök képviselte értéket, mely kettő részből tevődik össze: a szerverek, hálózati eszközök értékes vagyonelemek, valamint a tárolt adatok is értéket képviselnek. Következésképpen az adatközpontokban jelen vannak vagyonvédelmi eszközök is a magas szintű létesítményi biztonság érdekében [38]. Ezen a ponton érdemes megemlíteni azon speciális védelmi eszközöket, melyek az IT eszközöket védelmezik a távolról való illetéktelen hozzáférés-, vagy az azok feletti irányítás megszerzése ellen [39]. Érthető tehát az egy helyen koncentrálódó, eltérő célú IT eszközök magas száma. Sándor és Nagy szerint egy adatközpont tűzkockázatát meghatározó tényező a szervertermek telítettsége a hőtermeléséből fakadóan, ugyanis az el nem vezetett hő okozta túlmelegedés növeli az elektromos tűzesetek bekövetkezési valószínűségét [40].

Az IT eszközök száma és az áramellátás biztosítása miatt az adatközpontokban a kábelek nagy mértékű jelenlétét is említeni kell. Az elektromos kábelek túlterhelés hatására felmelegednek, mely jelenség tüzet is képes okozni [41]. Már a gyulladási hőmérséklet alatt is képes károsodni a vezeték műanyag burkolata, és olyan folyamat kezdődik, mely során éghető gáz szabadul fel, fokozva a tűz kockázatát.

A túlmelegedés mellett tűzesetet indukálhat akkumulátor-probléma is. A folyamatos rendelkezésre állás érdekében az IT eszközök folyamatos áramellátását biztosítani szükséges, így alapvető feladat az akkumulátorok telepítése, szünetmentes tápellátási megoldás kiépítése. Az akkumulátorok tűzveszélyességére azonban már több eset is felhívta a figyelmet (pl. [42] és [43]).

Az adatközponti tűzvédelem tervezésekor figyelembe kell venni az IT eszközök magas számát. Mivel a vízzel oltó rendszerek (sprinkler) és a habbal oltó rendszerek az IT eszközöket károsíthatják, olyan alternatív megoldásokat kell alkalmazni, melyek a hűtés, illetve az oxigén kiszorítása során nem károsítják ezen IT eszközöket. Figyelembe kell venni ugyanis, hogy a fentebb említettek szerint az IT eszközök saját értékén túl a tárolt adatok is jelentőséggel bírnak, így összességében nagyon magas a védendő IT eszközök értéke.

Az adatközpontok további sajátosságának mondható, hogy egyes részeiben nem tartózkodik személyzet állandóan, csak alkalmi jelleggel, például karbantartás vagy eszközcsere idejére. Fizikailag és logikailag is elkülönülnek tehát a munkavállalók irodahelyiségei, a vezérlőtermek, és az IT eszközök üzemelési helyiségei, valamint az áramellátást biztosító

eszközök üzemelési helyiségei. Tűz kockázatának szempontjából is különböznek ezen helyiségek, így a tűzvédelem szempontjából is eltérések lehetnek, például irodahelyiségbe telepíthető vízzel oltó tűzoltó eszköz is, míg szerverteremben ezt a megoldást kerülni javasolt.

ADATKÖZPONTOK TŰZVÉDELMÉNEK KUTATÁSA A NEMZETKÖZI TUDOMÁNYOS SZAKIRODALOM ALAPJÁN

A kutatási célok és módszerek részben leírt szakirodalom-kutatás során feldolgozott tudományos cikkek eredményei az alábbiak szerint foglalhatóak össze.

Badhe és szerzőtársai 2025-ben közzétett tanulmányukban az adatközpontokban termelődő hő- és az IT eszközök működésük közbeni melegedésének a problémájára magukban az elektronikai eszközökben kerestek választ [44]. Olyan konstrukciós megoldást javasolnak, mely során LTCC kerámialapot integrálnak heterogén architektúrájú csipekre a termikus érintkezés kiküszöbölése érdekében, mellyel a hűtés hatékonysága növelhető. Prototípussal végzett kísérletükben kevesebb hűtő levegőre volt szükség, mint a hasonló teljesítményű Intel alátétlemez esetén.

Kim 2026-os cikkében olyan fűtési-, szellőztetési- és hűtési rendszert javasolt [45], amellyel moduláris, automatizációval integrált (emberi beavatkozás nélkül működtethető) füstmentesítő rendszer alakítható ki irányítóhelyiségekben. A már üzemelő tűzvédelmi rendszerek mellé gyorsan telepíthető megoldása belélegezhető levegőt biztosít a padlószinthez közel, ami az emberélet megóvását szolgálja.

Kareck és szerzőtársai 2026-os tanulmányukban az adatközponti tűzvédelem fokozására a megfelelő kockázatértékelést javasolják [46]. Módszertanukban figyelembe veszik a lehetséges kiváltó okokat, mint a túlfeszültség, az akkumulátor-probléma, a túlmelegedés és emberi hiba. Abból kiindulva, hogy mind a tűzvédelmi eszközök, mind az IT eszközök folyamatosan fejlődnek, a megtörtént tűzesetekből levont tanulságok felhasználása fontos eleme módszertanuknak.

Liang szerzőtársaival 2025-ben megjelentetett cikkükben az adatközpontokban is alkalmazott kábelek FR-PE (tűzgátló polimer) szigetelőanyagának tulajdonságaiban túláram hatására bekövetkező változásokat vizsgálták [47]. Túláram hatására a vezetőanyag melegedéséből fakadóan melegszik a szigetelő anyag is. Ez a hőmérséklet-emelkedés indukálhatja a szigetelőanyag polimerláncainak hasadását, a keresztkötött polimerek depolimerizációját és gyúlékony gázok keletkezését. A tanulmány szerzői szerint ezen folyamat mélyebb megértése az adatközpontok tűzvédelmének fokozását segítheti elő a tűz kockázatának pontosabb értékelése által.

Newman és szerzőtársai 2013-as publikációjukban adatközpontokban füstkár következményeként azonosítottak kettő esetet: a szivárgó áram kialakulását és a felületet károsítót (korrózióhoz vezetőt) [48]. Kísérletükben polikarbonát égésekor keletkező füst IT eszközök belsejében lerakódó maradványa okozta a legnagyobb mértékű áramszivárgást, míg a PVC égésekor keletkező füst eredményezte a legnagyobb mértékű korróziót a keletkező hidrogén-klorid miatt. Természetesen az áramszivárgás- és a korrózió mértéke a lerakódó füstmaradvány mennyiségével egyenesen arányos, de az elmondható, hogy potenciálisan kétféleképpen károsíthatja az IT eszközöket, illetve növelheti meg egy további tűz kockázatát, hiszen a szivárgó áram hőtermeléssel jár.

Yin szerzőtársaival 2026-ban publikált tanulmányukban az adatközpontokban széles körben használt előre gyártott, heptafluorpropán tűzoltó rendszer működését elemezte a

rendszer optimális beállításának támogatása érdekében [49]. Mivel a heptafluorpropán tiszta, elektromosan nem vezető és maga után maradványt nem hagyó gáz, alkalmas elektronikai berendezések, IT eszközök tűzvédelmére. Az ezen gázt használó tűzoltó rendszerek oltási hatékonyságát két tényező befolyásolja: a hőelnyelés és a gáz örvénylő áramlása. A kutatási mérések alapján kijelenthető, hogy a heptafluorpropán gáz kibocsátása olyan mértékű hőelnyeléssel jár a gáz terjedésének irányában, hogy ott a hőmérséklet akár -33 Celsius fokra is lehűlhet. A kutatás során vizsgálták a gázkifúvás magasságának hatását a tűzoltó képességre. Eredményük szerint a fúvókák optimális magassága 1,925 m, ekkor maximális ugyanis a hűtő hatás. A fúvókák további magasságának növelésével láthatóvá vált a természetes konvekció intenzitásának csökkenése, hiszen az IT eszközökhöz már kisebb sűrűségű heptafluorpropán gáz érkezett a tűzoltó rendszer működésbe lépésének kezdetén, így - a kezdeti időben - a hőelnyelési képesség is csökkent volt.

Zeng kutatótársaival 2021-ben megjelent cikkükben az IT eszközök tápellátását biztosító kábelek és az adatátviteli kábelek külső borításának éghetőségét vizsgálták [50]. Méréseik igazolták a PVC borítású kábelek égésekor keletkező gázok korrodáló voltát, míg az eredmények alapján az LSZH (alacsony füstkibocsátású halogénmentes) kábelek égésekor keletkező gázok nem, vagy csak csekély mértékben vezethetnek az elektronikai eszközök korróziójához. Az éghetőség szempontjából a vizsgált kábelek ellenállónak bizonyultak a lángterjedéssel szemben, kivéve a 6 mm átmérőjű, PVC külső borítású és magas polietilén tartalmú szigetelő burkolattal rendelkező kábelt, mely tűzállóságát a teszteredmények megkérdőjelezik.

KÖVETKEZTETÉSEK

A fentiek szerinti nemzetközi szakirodalmi kutatásunk alapján az egyértelműen megállapítható, hogy az adatközponti tűzvédelem témájával foglalkozik a nemzetközi tudományos közösség, megjelennek a témakör különböző kérdéseit tárgyaló publikációk. Lehetséges tehát ezen publikációkból következtetéseket levonni, bár azt meg kell jegyezni, hogy ez a kutatási terület a vizsgált adatbázisban elérhető publikációk száma alapján kicsinek mondható, ezért a növekvő bár, de még mindig kevés számú tanulmányból fakadóan a következtetésekkel óvatosnak kell lenni.

Első, és talán legfontosabb következtetésként kijelenthető, hogy a téma fontosságát és aktualitását elismerte a tudományos közösség, ami összhangban áll a nemzetközi hírekben megjelenő, világszerte bekövetkező adatközponti tűzesetekkel. A vizsgált publikációk 71%-a 2025-ben vagy 2026-ban jelent meg. Ez a terület tehát kutatott, a problémákra válasz keresését a nemzetközi tudományos közösség aktuálisnak tartja, a vonatkozó tudományos kutatások száma jelenleg növekvő ütemben gyarapszik.

További következtetéseink során az adatközpontok tűzvédelmi szempontú sajátosságaiból kiindulva azt vizsgáljuk, hogy a nemzetközi kutatási eredmények hogyan kapcsolódnak ezen specialitásokhoz? Tűzvédelmi szempontból az adatközpontok sajátossága 1) az IT eszközök és elektromos berendezések hőtermelése; 2) az elektromos kábelek gyulladásának fokozott veszélye; 3) az akkumulátorok tűzveszélyessége; 4) az IT eszközöket nem károsító oltórendszerek iránti igény; 5) az eltérő tűzvédelmi kockázatú és megoldást igénylő helyiségek.

1. Kijelenthetjük, hogy az adatközponti hőtermelés okozta problémával a tudományos közösség napjainkban is foglalkozik: a vizsgált publikációk közül [44] olyan megoldást javasol az IT eszközök felépítésére, mely kevesebb hőtermeléssel jár. Ugyanakkor az épület hűtési lehetőségeit elemző tanulmányt nem találtunk kutatásunk során, ami alapján csak annyit jelenthetünk ki, hogy ez a kérdéskör tűzvédelmi szempontból eddig nem kutatott. Mindez alapján az nem zárható ki az, hogy az adatközponti hűtés témájának zajlik más szempontból, például energiahatékonyság szempontjából történő kutatása. Ennek megállapítása egy másik - jövőbeli - kutatás eredménye lehet.
2. Igazolt az adatközpontokban nagy mennyiségben jelen lévő elektromos kábelek tűzveszélyessége, illetve azoknak tűz kockázatát növelő hatása. Fenti kutatásunk alapján elmondható, hogy ezt a problémát a nemzetközi tudományos közösség vizsgálja, hiszen vonatkozó kutatási eredmények megjelennek. [47] és [50] egyaránt megállapította, hogy a vezetőanyag melegedéséből fakadóan melegszik a szigetelőanyag is, ami indukálhatja a műanyag szigetelőanyag polimerláncainak hasadását, a keresztkötött polimerek depolimerizációját és gyúlékony gázok keletkezését. Ezen eredmények további kutatásoknak ágyaznak meg, és a hőnek és tűznek ellenálló elektromos kábelek kifejlesztésének irányába való haladásra engednek következtetni. [48] az elektromos kábelek melegedésének és égésének folyamatát, illetve hatását tanulmányozta. Ez a tudománynak nem csak az előbb említett irányba való haladását mutatja, hanem még arra is következtethetünk, hogy a megkezdődött a kábelek égésének elektronikai eszközökre gyakorolt káros hatásának mérséklésére vonatkozó lehetőségek kutatása.
3. Akkumulátorok tűzveszélyességének problémájával foglalkozó tanulmányt nem találtunk kutatásunk során. Ennek a jelenségnek a széles körben ismert volta, továbbá a bekövetkezett tűzesetek példája valószínűsíti, hogy a tudományos közösség kutatja ezen kérdéskört, de vagy nem jelent még meg kutatási eredmény, vagy nem adatközpontokra fókuszáló kutatások zajlanak. Ennek megállapítására jelen kutatásunk elégtelen, így további szakirodalmi kutatás szükségeltetik.
4. Adatközpontok tűzvédelmi szempontú sajátossága az egy helyen koncentrálódó IT eszközök magas száma, melynek következtében speciális tűzoltási megoldások szükségesek. [49] az adatközpontokban széles körben használt előre gyártott, heptafluorpropán tűzoltó rendszer működését elemezte és határozta meg a rendszer optimális beállítását. Mivel a heptafluorpropán nem károsítja az elektronikai eszközöket, adatközpontokban használható, így az optimális beállítás gyakorlatban alkalmazható kutatási eredménynek tekinthető. Ugyanakkor az adatközpontok terjedését figyelembe véve valószínűsíthető, hogy az eltérő építészeti megoldások okán további kutatások válnak szükségessé, mindenesetre az kijelenthető, hogy a tudományos közösség gyakorlatban alkalmazható speciális tűzoltási rendszerre vonatkozó eredményt publikált 2026-ban.
5. Az adatközpontok eltérő felépítésűek lehetnek, azonban az közös bennük, hogy egymástól fizikailag és logikailag is elkülönülő helyiségekre bonthatóak, melyek tűz kockázatának szempontjából is eltérő tulajdonságokat mutatnak. [45] olyan fűtési-, szellőztetési- és hűtési rendszert javasolt irányítóhelyiségek számára, mely az

ilyen célú helyiségek füstmentesítését és hűtését lehet képes biztosítani. Az ezt az adatközpontokban is alkalmazható megoldást bemutató publikáció igazolja, hogy a nemzetközi tudományos közösség foglalkozik a katasztrófahelyzetekben még fontosabbá váló vezérlőtermek, irányítóhelyiségek tűzvédelmi kérdéseivel. Ugyanakkor az is kijelenthető, hogy ezen tanulmány csak egy szempontot vizsgált, további, ide illeszkedő publikációt nem találtunk kutatásunk során, így ezen helyiségek sajátosságaiból fakadó tűzvédelmi tényezők feltárása a tudományos közösség számára további feladatot jelenthet.

Az adatközpontok sajátosságai mentén levont következtetések után felmerül a kérdés, hogy a tűz kockázatának értékelése terén is szükséges-e, javasolható-e speciális megoldás? A 2026-ban megjelent [46] egy konkrét kockázatértékelési módszertant javasol adatközponti tűzvédelemre, mely figyelembe veszi a fent említett sajátosságok mellett a megtörtént incidensekből levonható tanulságokat is. Ezek alapján kijelenthető, hogy a nemzetközi tudományos publikáció gyakorlati alkalmazásra javasol egy, az adatközponti tűzvédelem specialitásaihoz igazodó kockázatértékelési módszertant. Hozzá kell tenni azonban, hogy ennek a 2026-ban publikált módszertannak a gyakorlati alkalmazásából nem állhat rendelkezésre kellő számú tapasztalat, így annak vizsgálata jövőbeli kutatási témául szolgálhat.

ÖSSZEFOGLALÁS

A tűz elleni védekezés fontossága vitathatatlan, különösen az IT szolgáltatások miatt kiemelt jelentőségű adatközpontok esetében, melyek némelyike a kritikus infrastruktúra részévé válik. Az adatközponti tűzvédelem szükségességét világszerte megtörtént incidensek is alátámasztják.

Az adatközpontok sajátosságait is figyelembe vevő tűzvédelmi kérdéskör jelentőségét a nemzetközi tudományos közösség felismerte, a témában az elmúlt években növekvő számú publikáció jelenik meg. Az adatközponti tűzvédelemmel foglalkozó nemzetközi tudományos cikkek áttekintése után több következtetést is levontunk. Legfontosabb következtetésként kijelenthető, hogy a téma aktualitását felismerte a tudományos közösség, ami összhangban áll a nemzetközi hírekben megjelenő, világszerte bekövetkező adatközponti tűzesetekkel. A vizsgált publikációk 71%-a 2025-ben vagy 2026-ban jelent meg. Ez a terület tehát kutatott, a vonatkozó tudományos kutatások számossága jelenleg növekvő ütemben gyarapszik. Ugyanakkor a jelenleg kevés számú tanulmány alapján az is feltételezhető, hogy ezen kutatások még gyerekcipőben járnak, a gyakorlatban is használható eredményekre még várni kell. Véleményünk szerint az adatközponti tűzvédelem területét továbbra is kutatni szükséges.

FELHASZNÁLT IRODALOM

[1] Banga, K., Harbansh, P., Singh, S. „Digitalisation and Structural Change: Evidence from Cross-Country Analysis” *JOURNAL OF DIGITAL ECONOMY*, 2026, https://doi.org/10.1016/j.jdec.2026.03.003

[2] Dobos O., Csiszárik-Kocsir Á. „Project-oriented perceptions of research, development and innovation in Hungarian, Polish and Romanian enterprises” *TRANSFORMATIONS IN BUSINESS & ECONOMICS*, 24(1), 2025, https://www.transformations.knf.vu.lt/64/article/proj

[3] Altaleb, H., Rajnai Z. „5G Infrastructure Standardization, Integration, Industry 4.0 Applications in EU Precisely Germany, and the Future of Industry 5.0 and 6G: A Comprehensive Overview”, In: Kovács, Tünde Anna; Stadler, Róbert Gábor; Daruka, Norbert (szerk.) *The Impact of the Energy Dependency on Critical Infrastructure Protection : Proceedings of the 5th International Conference on Central European Critical Infrastructure Protection (ICCECIP 2023)*, Cham, Svájc : Springer Nature Switzerland (2025), https://doi.org/10.1007/978-3-031-78544-3_7

[4] Fabricius-Ferke Gy. „Jönnek helyettünk a robotok? Rutinszerű, vagy egyedi munka; számítógépes szoftverek, vagy kreatív mesterséges intelligencia?” *POLGÁRI SZEMLE*, 20(1-3), 2024, https://doi.org/10.24307/psz.2024.0815

[5] Forgács A., Lukács J., Csiszárik-Kocsir Á., Horváth R. „Az internetes vásárlás magatartásának vizsgálata fuzzy következtetési rendszer segítségével” *POLGÁRI SZEMLE*, 20(4-6), 2024, https://polgariszemle.hu/images/content/pdf/1024307psz20241110.pdf

[6] Yu, Z., Liu, J. „The digital revolution in banking: Unpacking risk management in the age of transformation” *INTERNATIONAL REVIEW OF ECONOMICS & FINANCE*, Vol 103, 2025, https://doi.org/10.1016/j.iref.2025.104444

[7] Marosi Gy. „Digitalisation and Innovation in Public Administration” *POLGÁRI SZEMLE*, 21(4-6), 2025, https://doi.org/10.24307/psz.2025.0915

[8] Codreanu, A., Vasilescu, C. „Distance Learning or Resident Educational and Training Programs? Possible Solutions to the Effectiveness Dilemma in Military Education” *ROMANIAN MILITARY THINKING*, 2024(1), 2024, https://doi.org/10.55535/RMT.2024.1.10

[9] Heitlerné Lehoczky M., Kollár Cs. „A mesterséges intelligencia múltja, jelene és jövője a senior és a junior szakértők szemszögéből: 1. rész” *BIZTONSÁGTUDOMÁNYI SZEMLE,* 4(1), 2022, https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/208/184

[10] Scholtz E., Pántya P. „A mestersége intelligencia fejlődése és felhasználhatósága a katasztrófavédelemben” *POLGÁRI VÉDELMI SZEMLE*, 18, 2026, https://mpvsz.hu/pv_szemlek/pvszemle2026/index.html

[11] Mihajlović, I., Petrović, N., Spasojević Brkić, V., Milijić, N. „Artificial intelligence as a tool for item reduction in an organizational resilience questionnaire” *INTERNATIONAL JOURNAL OF OCCUPATIONAL SAFETY AND ERGONOMICS*, 31(140), 2025, https://doi.org/10.1080/10803548.2025.2465165

[12] Csercsa K., Rajnai Z. „Adatvédelem és információbiztonság: az online térben fellelhető veszélyforrások, adathalászati módszerek (social engineering)” *BIZTONSÁGTUDOMÁNYI SZEMLE*, 7(2), 2025, https://doi.org/10.12700/btsz.2025.7.2.49

[13] Kiss A., Kollár Cs. „Az információbiztonság időszerű kérdései a magyarországi kkvk körében” *SCIENTIA ET SECURITAS*, 4(2), 2024, https://doi.org/10.1556/112.2023.00166

[14] Besenyő J., Őszi A. „Sensing From the Skies: A Comprehensive Analysis of the Latest Sensors on Drones” *JOURNAL OF ROBOTICS*, 2025 : 1, 2025, https://doi.org/10.1155/joro/3896195
[15] JP Morgan. „Business Leaders Outlook - Leaders forge ahead in 2026”, 2026, https://www.jpmorgan.com/insights/markets-and-economy/business-leaders-outlook/2026-us-business-leaders-outlook
[16] Chase. „2026 Business Leaders Outlook: Reflections and predictions for what’s next”, https://www.chase.com/business/knowledge-center/manage/blo-2026
[17] Marr, B. „5 Business Trends Every Company Must Prepare For In 2026” 2025, https://www.forbes.com/sites/bernardmarr/2025/11/18/5-business-trends-every-company-must-prepare-for-in-2026/
[18] Michelberger P. „Folyamatalapú, szabványos irányítási rendszerek a biztonságos és rugalmas vállalati működésért” *SCIENTIA ET SECURITAS*, 3(4), 2023, https://doi.org/10.1556/112.2023.00136
[19] Krepuska A., Nagy R. „Tűzvédelem gazdasági vonatkozásai multinacionális környezetben” *BIZTONSÁGTUDOMÁNYI SZEMLE*, 7(2), 2025, https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/552
[20] Data Center Knowledge. „Digital Edge to Develop 500 MW Data Center Campus in Indonesia” 2026, https://www.datacenterknowledge.com/data-center-construction/digital-edge-to-develop-500-mw-data-center-campus-in-indonesia
[21] Data Center Knowledge. „Oracle Eyes $50B for AI Infrastructure in 2026” 2026, https://www.datacenterknowledge.com/infrastructure/oracle-eyes-50-billion-for-ai-infrastructure-in-2026
[22] Data Center Knowledge. „New Data Center Developments: February 2026”, 2026, https://www.datacenterknowledge.com/data-center-construction/new-data-center-developments-february-2026#European%20Data%20Center%20Developments
[23] Data Center Knowledge. „Moody’s: $3 Trillion Data Center Investment by 2030 Amid Power Challenges”, 2026, https://www.datacenterknowledge.com/energy-power-supply/moody-s-3-trillion-data-center-investment-by-2030-amid-power-challenges
[24] Berek L., Steiner A. „A térfigyelő kamerarendszer helye, szerepe a bűnmegelőzésben” *BELÜGYI SZEMLE*, 73(5), 2025, https://belugyiszemlejournal.org/index.php/belugyi-szemle/article/view/2102
[25] Besenyő J., Todorović, B. „Influence of security requirements to engineering in process industry” In: SMEITS - SMEITS (szerk.) *38. Međunarodni kongres o procesnoj industriji*. Online kiadás, Nemzetközi : Savez masinskih i elektrotehnickih inzenjera i tehnicara Srbije (SMEITS) (2025) pp. 191-198., https://izdanja.smeits.rs/index.php/ptk/article/view/8221/8459
[26] Muhoray Á. „A védelmi és biztonsági események, a katasztrófák következményei felszámolásában a fokozatosság elve” *POLGÁRI VÉDELMI SZEMLE*, 17, 2025, https://mpvsz.hu/pv_szemlek/pvszemle2025/index.html
[27] Vass Gy., Ambrusz J., Restás Á., Varga F., Kátai-Urbán L. „A katasztrófavédelmi kutatások eredményei és fejlesztése a rendészettudomány rendszerében” *BELÜGYI SZEMLE*, 72(5), 2024, https://doi.org/10.38146/BSZ-AJIA.2024.v72.i5.pp815-833
[28] Bojtos Z., Nagy R. „Some aspects of a complex urban defence” In: Ćeranić, Predrag (szerk.) *ЗБОРНИК РАДОВА VI међународни научни скуп „Савремени изазови и*

прије безбједности" Бања Лука, Република Српска, БиХ, 27. март 2026. године = ZBORNIK RADOVA VI međunarodni naučni skup „Savremeni izazovi i prijetnje bezbjednosti" Banja Luka, Republika Srpska, BiH, 27. mart 2026. godine, Banja Luka, Bosznia-Hercegovina : Univerzitet u Banjoj Luci, Fakultet bezbjednosnih nauka (2026)

[29] Sikimić, M. „Security of European critical infrastructures outside the European Union: a review of the Western Balkans national laws" *INSIGHTS INTO REGIONAL DEVELOPMENT*, 4(2), 2022, https://doi.org/10.9770/ird.2022.4.2(5)

[30] Bálint K., Berek T. „Possible Computerized, Modern Solutions for Fire Protection of the Universities in Subotica, Serbia" In: Borsos, É; Horák, R; Kovács, C; Némesztovszky, Zs (szerk.) *Mobilitás : A Magyar Tannyelvű Tanítóképző Kar tudományos konferenciáinak tanulmánygyűjteménye*. Szabadka, Szerbia : Újvidéki Egyetem Magyar Tannyelvű Tanítóképző Kar (2019) 679 p. https://magister.uns.ac.rs/files/kiadvanyok/konf2019/ConfSubotica2019.pdf#page=42

[31] Mihály I., Bérczi L., Bognár B., Kátai-Urbán M., Tóth L., Kátai-Urbán L., Vass Gy. Varga F. „Experimental Study to Determine the Leakage Area of Single-Leaf Smoke Control Doors in the Design of Pressure Differential Systems" *FIRE*, 8(1), 2025, https://doi.org/10.3390/fire8010005

[32] Restás Á. „A légi tűzoltás hatékonyságának tűzoltástaktikai megközelítése" *HADITECHNIKA*, 58(2), 2024, https://honvedelem.hu/kiadvanyok/haditechnika-2024-2-szam.html

[33] Érces G., Tóth R., Vass Gy., Varga F. „Developing fire safety visualised by augmented reality" POLGÁRI VÉDELMI SZEMLE, 17, 2025, https://mpvsz.hu/pv_szemlek/pvszemle2025/index.html

[34] Data Center Knowledge „How to Prevent Data Center Fires: Lessons from the Biggest Incidents" 2024, https://www.datacenterknowledge.com/outages/how-to-prevent-data-center-fires-lessons-from-the-biggest-incidents

[35] CNA „Fire at Loyang data centre, SCDF operations still ongoing after a day" 2024, https://www.channelnewsasia.com/singapore/fire-loyang-digital-realty-data-centre-scdf-operation-4599316

[36] BDRShield „South Korea Data Center Fire: A Critical Wake-Up Call for Data Resilience" 2025, https://www.bdrshield.com/blog/south-korea-data-center-fire-a-critical-wake-up-call-for-data-resilience/

[37] Zhang, Y., Li, H., Wang, S. „The global energy impact of raising the space temperature for high-temperature data centers" *CELL REPORTS PHYSICAL SCIENCE*, 4(10), 2023, https://doi.org/10.1016/j.xcrp.2023.101624

[38] Horváth T. „Design Principles of a Physical Protection System for Data Centres: Essential Requirements for the Security Staff in the Physical Protection System" *MAGYAR RENDÉSZET*, 20(2), 2020, https://doi.org/10.32577/mr.2020.2.9

[39] Gulyás O. „A kiberbiztonság és a banki kibervédelem fejlődése napjainkig" *BIZTONSÁGTUDOMÁNYI SZEMLE*, 4(2), 2022, https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/218

[40] Sándor B., Nagy R. „Adatközpontok tűzbiztonságának vizsgálata" *VÉDELEM TUDOMÁNY*, 5(1), 2020, https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13375

[41] Gyöngyössy É.E. „Fire Hazard of Fire-Resistant Cables Below the Ignition Point” *MŰSZAKI KATONAI KÖZLÖNY*, 35(3-4), 2026, http://doi.org/10.32562/mkk.2025.3-4.9
[42] Trabelsi, O., Kovács T. A. „A lítium-ion akkumulátorok tűzoltása” *MŰSZAKI TUDOMÁNYOS KÖZLEMÉNYEK*, 20(20), 2024, https://doi.org/10.33895/mtk-2024.20.16
[43] Pántya P. „A li-ion akkumulátorok tűzoltásával kapcsolatos kutatási tapasztalatok, a tűzoltói beavatkozás lehetőségei” *VÉDELEM TUDOMÁNY*, 8(2), 2023, https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13493/10935
[44] Badhe, P. et al. „Experimental and numerical investigation of LTCC-based liquid cold plate for high-performance computing processors” *APPLIED THERMAL ENGINEERING*, 279, 2025, https://doi.org/10.1016/j.applthermaleng.2025.128052
[45] Kim, B. „A smart HVAC retrofit system to improve fire safety in mission-critical facilities” *CASE STUDIES IN THERMAL ENGINEERING*, 77, 2026, https://doi.org/10.1016/j.csite.2025.107330
[46] Kareck, T.L. et al. „From incident to insight: Fire risk in modern data centers” *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, 100, 2026, https://doi.org/10.1016/j.jlp.2025.105890
[47] Liang, S. et al. „Pyrolysis and gas evolution behavior of overloaded flame-retardant polyethylene cable insulation” *CASE STUDIES IN THERMAL ENGINEERING*, 75, 2025, https://doi.org/10.1016/j.csite.2025.107223
[48] Newman, J.S., Su, P., Yee, G.G., Chivukula, S. „Development of smoke corrosion and leakage current damage functions” *FIRE SAFETY JOURNAL*, 61, 2013, http://dx.doi.org/10.1016/j.firesaf.2013.08.016
[49] Yin, Q. et al. „Field distribution characteristics and performance optimization of heptafluoropropane spraying and stratification in prefabricated fire-extinguishing systems” *CASE STUDIES IN THERMAL ENGINEERING*, 81, 2026, https://doi.org/10.1016/j.csite.2026.107935
[50] Zeng, D. et al. „Evaluation of flammability and smoke corrosivity of data/power cables used in data centers” *FIRE SAFETY JOURNAL*, 120, 2021, https://doi.org/10.1016/j.firesaf.2020.103094