

CHALLENGES OF MODERN SECURITY TECHNOLOGY: EQUIPMENT LIFESPAN AND TECHNOLOGICAL DEVELOPMENT**A MODERN BIZTONSÁGTECHNIKA KIHÍVÁSAI: ESZKÖZÉLETTARTAM ÉS TECHNOLÓGIAI FEJLŐDÉSE**ANDRISKA Gergő¹**Abstract**

This study aims to explore the relationship between the lifespan of security technology systems, their technological advancement, and the economic return on investment. Due to rapid innovation, both hardware and software developments significantly impact the efficiency and applicability of these systems. The increasing use of artificial intelligence opens new possibilities, though concerns remain regarding its reliability and autonomous operation. Hardware advancements – such as sensors, image processing units, and control systems – represent progress, but their economic justification is not always evident. The research emphasizes that implementing technological innovations must be based on a thorough cost-benefit analysis, with attention to the full lifecycle of the systems.

Keywords

security technology, service life, obsolescence, technological development, investment return, life cycle management

Absztrakt

A tanulmány célja a biztonságtechnikai eszközök élettartama, technológiai fejlődése és a beruházások gazdasági megtérülése közötti összefüggések vizsgálata. A gyors technológiai fejlődés következtében mind hardveres, mind szoftveres téren folyamatosan jelennek meg új fejlesztések, amelyek hatással vannak a biztonságtechnikai rendszerek hatékonyságára és alkalmazhatóságára. A mesterséges intelligencia egyre szélesebb körű alkalmazása új lehetőségeket kínál, ugyanakkor kérdéses a megbízhatósága és önálló alkalmazhatósága. A hardverfejlesztések – mint az érzékelők, képfeldolgozó egységek és vezérlőrendszerek – jelentős előrelépést jelentenek, ám gazdaságossági szempontból nem minden esetben indokoltak. A kutatás rávilágít arra, hogy a technológiai újítások bevezetésének költség-haszon elemzésen kell alapulnia, figyelembe véve a rendszerek teljes életciklusát.

Kulcsszavak

biztonságtechnika, élettartam, elavulás, technológiai fejlődés, megtérülés, életciklus-menedzsment

¹ andriska.gergo96@gmail.com | ORCID: 0000-0002-6318-4084 | University student, Obuda University Bánki Donát Faculty of Mechanical and Safety Engineering | Egyetemi hallgató, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A biztonságtechnikai rendszerek alkalmazása az elmúlt évtizedekben jelentős technológiai fejlődésen ment keresztül, amelynek eredményeként nőtt a védelmi rendszerek hatékonysága és bővültek a technológiai lehetőségek. Az olyan rendszerek, mint a megfigyelő kamerák, beléptető rendszerek, valamint tűz- és behatolásjelző berendezések, nemcsak a fizikai biztonság szavatolására szolgálnak, hanem adatokat is biztosítanak az események elemzéséhez és a preventív intézkedések kidolgozásához. Az eszközök műszaki paramétereit és élettartama azonban jelentős eltéréseket mutat, és a gyors technológiai innovációk következtében gyakran az eszközök fizikai elhasználódása előtt technológiailag meghaladottá válnak.

Gazdasági szempontból kulcsfontosságú az eszközök megtérülési mutatóinak vizsgálata. Egy biztonságtechnikai beruházás akkor tekinthető eredményesnek, ha az eszköz teljes élettartama alatt a befektetett költségek és az elért biztonsági szint közötti arány optimális. A technológiai elavulás ugyanakkor rendszeres frissítéseket vagy teljes rendszer cseréjét teszi szükségessé, ami növeli a fenntartási költségeket. Ezért a vállalatok és intézmények számára elengedhetetlen, hogy stratégiai megközelítést alkalmazzanak a biztonságtechnikai rendszerek életciklus-menedzsmentjében.

Jelen kutatás célja a biztonságtechnikai eszközök jellemző élettartamának átfogó elemzése, az elavulás különböző formáinak azonosítása, valamint a technológiai fejlődés eszközcserékre és megtérülési ütemezésre gyakorolt hatásainak vizsgálata. A tanulmány arra törekszik, hogy feltárja, miként egyeztethetők össze a műszaki, biztonsági és gazdasági szempontok egy hosszú távon fenntartható biztonságtechnikai stratégia kialakítása érdekében.

TÖRTÉNETI ÁTTEKINTÉS (1970–2025)

A biztonságtechnikai eszközök fejlődését az elmúlt öt évtizedben jól körülhatárolható technológiai ugrások jellemezték, amelyek jelentősen befolyásolták az eszközök alkalmazhatóságát, elavulását és cseréjének ütemezését.

- **1973 – CCTV-rendszerek bevezetése a londoni metróban**

A londoni metróvonalakon 1973-ban telepítettek először analóg zártláncú kamera-rendszert (CCTV), amely fekete-fehér képet rögzített videokazettára. A rendszer célja kezdetben kizárólag a megfigyelés volt, automatizált funkciók vagy távoli hozzáférés nélkül.

- **1984 – HID első elektronikus beléptető rendszer**

A HID Corporation ekkor vezette be első nagyszabású mágneskártyás beléptető rendszerét vállalati környezetben. Ez forradalmasította az azonosítástechnikát, és kiváltotta a mechanikus kulcsokat az érzékeny objektumoknál.

- **1996 – Axis NetEye 200, az első IP-kamera**

Ebben az évben dobta piacra az Axis Communications a világ első IP-alapú kameráját, a NetEye 200-at. Ez a lépés alapozta meg a mai hálózati megfigyelőrendszerek elterjedését, amelyeknél már nem volt szükség közvetlen kábeles összeköttetésre a kamerák és a rögzítő között.

- **2008 – Milestone XProtect NVR-rendszer széles körű bevezetése**
A dán Milestone Systems 2008-tól kezdve ipari szinten is elérhetővé tette XProtect nevű, skálázható hálózati videómenedzsment szoftverét. Ez lehetővé tette az IP-alapú kamerák központosított, szoftveralapú kezelését, akár több ezer eszköz integrációjával.
- **2016 – Hikvision DeepinView: mesterséges intelligencia videóanalitikában**
A Hikvision 2016-ban jelentette meg DeepinView kameracsaládját, amely képes arcfelismerésre, viselkedéselemzésre és tömegszámlálásra. A mesterséges intelligencia ekkor kezdett gyakorlati jelentőséggel bírni a valós idejű incidensészlelésben.
- **2023 – Verkada: felhőalapú, IoT-integrált biztonsági platformok**
A Verkada és hasonló gyártók olyan felhőalapú megfigyelő rendszereket kínálnak, amelyek IoT-eszközöket (pl. szenzorok, beléptetők, videómodulok) egyetlen webes platformon kezelnek, prediktív riasztásokkal és teljesen távoli menedzsmenttel. Ez radikálisan csökkenti az on-site IT szükségletet.

Mint látható, a technológiai váltások (pl. analógról digitálisra, lokálisról hálózati vagy felhőalapú rendszerekre) kb. 10–12 évente új korszakot nyitottak a biztonságtechnikában.

A TÉMA ELMÉLETI ALAPJAI

A biztonságtechnikai rendszerek típusai és szerepük

A biztonságtechnikai rendszerek olyan komplex műszaki megoldások, amelyek célja az emberek, eszközök és adatok védelme különféle fenyegetésekkel – például illetéktelen behatolással, tűzzel, lopással vagy szabotázzsal – szemben. E rendszerek különösen kiemelt jelentőséggel bírnak a kritikus infrastruktúrák (KI) védelmében, ahol egy esetleges működésképtelenség nemcsak gazdasági, hanem társadalmi és nemzetbiztonsági következményekkel is járhat [1].

A biztonságtechnikai rendszerek az alábbi fő kategóriákba sorolhatók:

- **Megfigyelőrendszerek (CCTV/IP alapú):** Lehetővé teszik a folyamatos vagy eseményvezérelt vizuális megfigyelést. A modern rendszerek képesek mesterséges intelligencia alapú videóanalízisre, mozgásérzékelésre, arcfelismerésre, viselkedéselemzésre.
- **Beléptető rendszerek:** Feladata a hozzáférés szabályozása fizikai terekhez (pl. kártyás, biometrikus vagy PIN alapú rendszerek). Ezek kulcsszerepet játszanak a területre belépő személyek azonosításában és nyomon követésében.
- **Behatolásjelző rendszerek (IAS):** Olyan érzékelők összessége (pl. mozgás-, rezgés-, üvegtöréserzékelők), amelyek az illetéktelen behatolásokat detektálják és riasztást indítanak.
- **Tűz- és füstjelző rendszerek:** Elsődleges céljuk a korai észlelés és az életmentés, valamint az anyagi kár minimalizálása. Automatikus tűzjelzés, evakuációs irányítás és oltóberendezések aktiválása kapcsolódhat hozzájuk.
- **Integrált rendszerek:** Ezek a különféle rendszerek (pl. CCTV, beléptetés, IAS) egy közös platformon, egy egységes felügyeleti szoftveren keresztül működnek együtt, javítva a reakcióidőt és az adatfelhasználást.

Ezeknek a rendszerek hatékony működtetése és folyamatos fejlesztése elengedhetetlen a kritikus infrastruktúrák megbízható és biztonságos üzemeltetése érdekében. A nemzetközi szakirodalom is hangsúlyozza, hogy a biztonságtechnikai rendszerek integráltsági foka és technológiai színvonala közvetlenül befolyásolja az adott infrastruktúra kockázati kitettségét [2].

Az említett rendszerek nem csupán detektálnak, hanem adattárolási és -elemzési funkciókat is betöltenek. Ezáltal a biztonságtechnikai rendszerek az incidens utáni nyomozások, statisztikai elemzések és megelőző stratégiák kidolgozásának is alapját képezik.

AZ ESZKÖZÖK ÉLETTARTAMÁNAK MEGHATÁROZÓ TÉNYEZŐI ÉS AZ ELAVULÁS ELMÉLETE

A biztonságtechnikai rendszerek élettartama és elavulása szorosan összefüggő jelenségek, amelyek alapvetően befolyásolják a rendszerek megbízhatóságát, biztonsági szintjét és gazdasági fenntarthatóságát. Az élettartam alatt azt az időtartamot értjük, amely során az eszköz rendeltetés szerűen, biztonságosan és hatékonyan működik, míg az elavulás a fizikai, technológiai vagy funkcionális alkalmatlanság különböző formáit öleli fel. Az alábbiakban részletesen bemutatjuk az élettartamot meghatározó tényezőket, majd az elavulás elméletét, típusait és hatásait, hogy átfogó képet nyújtsunk e két terület kölcsönhatásáról és stratégiai jelentőségéről.

Az eszközök élettartamának meghatározó tényezői

A biztonságtechnikai eszközök élettartamát számos tényező befolyásolja, amelyek technológiai, környezeti, üzemeltetési és gyártói szempontból is megközelíthetők. Ezek pontos ismerete elengedhetetlen a fenntartási és fejlesztési döntések meghozatalához, valamint az optimális csereidőpont meghatározásához.

- **Műszaki paraméterek és beépített technológia:** Az eszközök élettartamának alapvető meghatározója a beépített technológia fejlettsége és a gyártási minőség. A korszerűbb, például IP-alapú rendszerek – amelyek önellenőrző funkciókkal, redundáns adatkezeléssel vagy szoftverfrissítési lehetőséggel rendelkeznek – általában hosszabb ideig képesek hatékonyan működni [1]. A hardveres elavulás jellemzően 5–10 év alatt következik be, míg a teljes funkcióvesztés többnyire 10–15 évnél jelentkezik [2]. Az olyan eszközök, mint az intelligens kamerák vagy tűzérzékelők, amelyek szoftveresen frissíthetők, hosszabb ideig maradhatnak relevánsak, mivel a szoftverfrissítések képesek lépést tartani a technológiai fejlődéssel.
- **Környezeti tényezők:** Az üzemelési környezet – például a hőmérséklet, páratartalom, por vagy korrózió – jelentős hatással van az eszközök élettartamára. Kültéri rendszerek, például térfigyelő kamerák, ki vannak téve szélsőséges időjárási viszonyoknak, UV-sugárzásnak és mechanikai behatásoknak, amelyek gyorsítják az anyagfáradást és az alkatrészek elhasználódását. Ezzel szemben a beltéri rendszerek stabilabb körülmények között hosszabb ideig maradnak üzembiztosak, különösen megfelelő karbantartás mellett. A környezeti tényezők figyelembevétele ezért kulcsfontosságú a rendszertervezés és az eszközválasztás során.

- **Karbantartás és használati gyakoriság:** A rendszeres karbantartás, például a megelőző ellenőrzések, tisztítás és szoftverfrissítések, jelentősen meghosszabbíthatja az eszközök élettartamát [3]. Az intenzív használat, például a 24/7 működés, gyorsíthatja az alkatrészek elhasználódását, különösen a mozgó elemek, mint például a kamerák forgatómotorjai vagy a beléptető rendszerek mágneszárvai esetében. Ezzel szemben a túllítkán használt eszközök elöregedése is problémát jelenthet, például az akkumulátorok kapacitásvesztése vagy az érintkezők oxidációja miatt. A karbantartási stratégia és az üzemeltetési szokások tehát közvetlenül befolyásolják az élettartamot.
- **Gyártói támogatás és frissítési ciklusok:** A gyártók által biztosított firmware- és szoftvertámogatás időtartama gyakran rövidebb, mint az eszköz fizikai élettartama. Különösen azoknál a rendszerknél amelyek hálózati kapcsolattal rendelkeznek. Az elavult szoftverek kiberbiztonsági kockázatokat hordoznak, mivel nem képesek megfelelni a legújabb biztonsági protokolloknak. A gyártói támogatás megszűnése után az eszköz technológiailag elavulttá válik, még ha fizikailag működőképes is. A frissítési ciklusok nyomon követése és a gyártói támogatási periódusok figyelembevétele ezért elengedhetetlen a hosszú távú működés biztosításához.

Az elavulás elmélete: típusok és hatások

Az elavulás a biztonságtechnikai rendszerek esetében nem csupán a fizikai elhasználódást jelenti, hanem egyre gyakrabban technológiai és funkcionális tényezőkben nyilvánul meg. Az elavulás mértéke és üteme közvetlenül befolyásolja az eszközök megbízhatóságát, biztonsági szintjét és gazdaságos üzemeltethetőségét, ezért elemzése kulcsfontosságú az életciklus-alapú tervezésben.

- **Fizikai elavulás:** A fizikai elavulás az anyagok természetes öregedéséből, mechanikai kopásából vagy elektronikai alkatrészek meghibásodásából fakad. Tipikus példái a szenzorok érzékenysége csökkenése, a kamerák képminőségének romlása vagy a mozgó alkatrészek – például motorok vagy relék – meghibásodása. Ez a folyamat különösen szembetűnő kültéri rendszereknél, ahol az időjárási viszonyok gyorsítják az elhasználódást. A fizikai elavulás fokozatos, és karbantartással – például alkatrészcserevel vagy tisztítással – időlegesen mérsékelhető, de az élettartam vége felé a karbantartási költségek jelentősen megnőhetnek.
- **Technológiai (erkölcsi) elavulás:** A technológiai elavulás során az eszközök ugyan még működőképesek, de funkcionalitásuk, kompatibilitásuk vagy biztonsági szintjük elmarad az aktuális iparági sztenderdektől [4]. Ez gyakran a szoftveres támogatás megszűnéséből, új szabványok bevezetéséből vagy a kiberbiztonsági követelmények szigorodásából ered. Például egy tíz évvel ezelőtti analóg CCTV-rendszer nem nyújt megfelelő képfelbontást vagy hálózati integrációt a mai igényekhez képest. Az olyan technológiák, mint az AI-alapú videóanalitika vagy a biometrikus azonosítás, különösen gyors elavulási ütemmel rendelkeznek, mivel az új algoritmusok és protokollok akár 3–4 év alatt elavulttá tehetik a rendszert.
- **Funkcionális elavulás:** A funkcionális elavulás akkor lép fel, amikor egy eszköz már nem képes kielégíteni a megváltozott működési vagy szervezeti igényeket [5]. Ez például akkor fordul elő, amikor egy vállalat új biztonsági protokollokat vezet

be, amelyekhez a meglévő rendszerek nem alkalmazkodnak, vagy amikor egy integrált platform bevezetése miatt a régebbi rendszerek kompatibilitási problémákkal szembesülnek. Egy beléptető rendszer, amely nem támogatja a többfaktoros azonosítást, funkcionálisan elavulttá válhat egy szigorúbb biztonsági környezetben, még ha technikailag működőképes is. A funkcionális elavulás szorosan összefügg a technológiai elavulással, de a kiváltó ok itt a használati kontextus változása.

- **Az elavulás hatása a rendszerbiztonságra és gazdaságosságra:** Az elavulás különböző típusai jelentős hatással vannak a biztonságtechnikai rendszerek teljesítményére és költséghatékonyságára. Az elavult rendszerek gyakran sebezhetőbbek, nem támogatják az új protokollokat, és nem képesek hatékonyan integrálódni más alrendszerrel, például tűzvédelmi vagy IT-biztonsági platformokkal, ezáltal növelve a rendszerszintű kockázatot [6]. Különösen a kritikus infrastruktúrák esetében súlyos gazdasági, társadalmi vagy nemzetbiztonsági következményekkel járhat egy elavult rendszer meghibásodása.

Gazdasági szempontból az elavulás növeli az üzemeltetési és karbantartási költségeket. A fizikai elavulás miatt gyakoribbá válik az alkatrészcsere vagy javítás, míg a technológiai és funkcionális elavulás gyakran a teljes rendszer cseréjét teszi szükségessé [7]. Az elavult rendszerek kevésbé hatékonyak, ami közvetett költségeket – például hosszabb reakcióidőt vagy alacsonyabb kockázatészlelési pontosságot – eredményez. Az élettartam és az elavulás közötti összefüggések elemzése ezért kulcsfontosságú a gazdasági és biztonsági szempontok összehangolásához.

- **Az élettartam és elavulás kölcsönhatása:** Az élettartamot befolyásoló tényezők és az elavulás típusai szoros kölcsönhatásban állnak. Például a környezeti tényezők gyorsíthatják a fizikai elavulást, míg a gyártói támogatás hiánya a technológiai elavulást erősíti. A karbantartás elhanyagolása mind a fizikai, mind a technológiai elavulást felgyorsíthatja, mivel a szoftverfrissítések elmaradása kiberbiztonsági kockázatokat, míg a mechanikai karbantartás hiánya az eszköz meghibásodását okozhatja. A funkcionális elavulás gyakran a technológiai elavulás következménye, de a szervezeti igények változása önmagában is indokolhatja a rendszer cseréjét, még ha az eszköz fizikailag és technikailag működőképes is.

A döntéshozatal során az élettartam és az elavulás közötti egyensúly megtalálása kulcsfontosságú. Az optimális csereidőpont meghatározása nem csupán az amortizációs szabályokon, hanem a kockázatértékelésen, a technológiai trendeken és a szervezet specifikus igényein is alapul [8]. Az életciklus-alapú tervezés, amely figyelembe veszi az élettartamot befolyásoló tényezőket és az elavulás különböző formáit, lehetővé teszi a fokozatos fejlesztések bevezetését, csökkentve a pénzügyi terheket és biztosítva a technológiai relevancia fenntartását.

ROI; TCO; CBA – AVAGY A MEGTÉRÜLÉS MATEMATIKÁJA

A biztonságtechnikai beruházások hatékonyságának vizsgálata a döntéshozatali folyamat elengedhetetlen eleme. Az értékelés során különböző gazdasági módszerek állnak rendelkezésre, melyek közül a leggyakrabban alkalmazottak: a megtérülési mutatók (ROI), a teljes élettartamköltség (TCO), valamint a költség–haszon elemzés (CBA). Ezek célja, hogy objektív alapot biztosítsanak a rendszerfejlesztési és csereidőztítési döntésekhez.

ROI (Return on Investment) - Beruházás-megtérülés

A ROI a beruházásból származó nettó nyereséget viszonyítja a beruházási költségekhez. A képlet a következő:

$$ROI = \left(\frac{B - K}{K} \right) * 100\%$$

ahol:

- B: a biztonságtechnikai rendszer által generált haszon (pl. csökkentett kárérték, biztosítási díjkedvezmény),
- K: a teljes beruházási költség.

A ROI egyszerű és gyors összehasonlítást tesz lehetővé, ugyanakkor nem veszi figyelembe az időértéket és a működési költségeket [7].

TCO (Total Cost of Ownership) - Teljes élettartamköltség

A TCO a rendszer teljes életciklusa során felmerülő összes költség számszerűsítésére szolgál. A képlet:

$$TCO = K_b + K_t + K_m + K_o + K_e$$

- K_b : beszerzési költség,
- K_t : telepítési és beüzemelési költség,
- K_m : működtetési költség (pl. energiafogyasztás, munkaerőköltség),
- K_o : karbantartási és javítási költség,
- K_e : selejtezési, csere- és leszerelési költség.

A TCO különösen alkalmas hosszú távú rendszerfejlesztések és integrált biztonságtechnikai beruházások gazdasági értékelésére [8].

CBA (Cost-Benefit Analysis) - Költség-haszon elemzés

A CBA a beruházás összes hasznát és költségét összeveti, figyelembe véve azok időbeli értékét. A nettó jelenérték (NPV) kiszámításának képlete:

$$NPV = \sum_{t=1}^n \frac{B_t + K_t}{(1 + r)^t}$$

ahol:

- B_t : a t-edik évben várható haszon,
- K_t : a t-edik évben felmerülő költség,
- r: diszkontráta,
- n: a projekt időtartama években.

Pozitív NPV esetén a beruházás gazdaságilag indokolt, míg negatív érték gazdaságtalanságra utal [9].

Technológiai innovációk hatása a megtérülésre

Az olyan új technológiák, mint a mesterséges intelligencia, prediktív analitika, IoT vagy felhőalapú rendszerek, rövid távon növelhetik a beruházási költségeket, azonban hosszú távon csökkenthetik az üzemeltetési és karbantartási kiadásokat. Ez befolyásolja a TCO

és ROI számításokat, így új számítási modellek és szimulációk alkalmazását teheti szükségessé a pénzügyi tervezés során [9].

Összehasonlító táblázat

	Jellemző élettartam	Technológiai el- avulás	Karbantartási igény	ROI (be- csült)	TCO szint (relatív)
Analóg CCTV kamera	6–8 év	Gyors	Alacsony	Alacsony (~3%)	Alacsony
IP-alapú kamera	7–10 év	Közepes	Közepes	Közepes (~7%)	Közepes
AI-alapú videóanalitika	4–6 év	Nagyon gyors	Magas	Magas (~12%)	Magas
Beléptető rendszer (RFID)	10–12 év	Lassú	Közepes	Közepes (~6%)	Közepes
Biometrikus beléptető	6–8 év	Közepes–gyors	Magas	Közepes (~8%)	Magas
Tűzjelző rendszer (optikai)	12–15 év	Lassú	Alacsony	Alacsony (~4%)	Közepes
Behatolásjelző rendszer	8–10 év	Közepes	Közepes	Közepes (~6%)	Közepes

1. táblázat Különböző biztonságtechnikai rendszerek élettartam-elavulás összegzése
(saját szerkesztés)

Elemzés és értelmezés

Az egyes eszköztípusok közötti különbségek nemcsak műszaki paramétereikben, hanem működtetési és gazdasági szempontjaikban is jelentősek. A saját elemzésem során négy fő kategóriát határoztam meg: műszaki időtállóság, technológiai elavulás, karbantartási igény, valamint beruházási megtérülés (ROI) és teljes élettartamköltség (TCO).

- **Műszaki időtállóság:** A tűzjelző rendszerek és RFID-alapú beléptetők kiemelkednek a hosszú élettartamukkal, amelyet egyszerű, jól bevált technológiájuknak és alacsony szoftverfüggőségüknek köszönhetnek. Az ilyen eszközök gyakran több mint egy évtizeden keresztül használatban maradnak, különösebb fejlesztés vagy korszerűsítés nélkül. Ezzel szemben a gyorsan fejlődő területeken – például a képfeldolgozás vagy biometrikus azonosítás – használt eszközök rövidebb időn belül morzsolódnak le technológiai szempontból, még ha fizikailag tovább is működőképesek.
- **Technológiai elavulás:** A technológiai avulás a mesterséges intelligencia alapú eszközöknél a leggyorsabb. Az új algoritmusok, szabványok és hálózati követelmények akár 3–4 év alatt elavulttá tehetnek egy korábban korszerű rendszert. Az IP-alapú eszközök esetében az erkölcsi elavulás általában 6–8 év között következik be, míg az analóg rendszerek már gyakorlatilag elavultnak tekinthetők. Saját értékelésem szerint ez az egyik legfontosabb tényező, amit a beszerzési döntések során figyelembe kell venni.
- **Karbantartási igény:** A kevésbé bonyolult rendszerek – mint például a passzív tűzjelzők vagy az analóg kamerák – karbantartási igénye alacsony, rendszerint csak alapvető működésellenőrzésre, tisztításra és tesztelésre van szükség. Ezzel szemben a szoftverintenzív rendszerek (pl. AI, biometria) rendszeres frissítést, konfigurálást,

esetenként rendszeres újratanítást igényelnek, ami szakemberi jelenlétet, magasabb költséget és szervezési ráfordítást jelent.

- **Megtérülés és költséghatékonyság:** A példaszámítás alapján kimutattam, hogy az AI-alapú rendszerek ugyan rövidebb élettartammal és magasabb TCO-val rendelkeznek, mégis nagyobb megtérülést biztosíthatnak, ha helyesen vannak beillesztve a védelemi struktúrába. Ez azonban csak akkor igaz, ha a működési környezet lehetővé teszi az automatizált kockázatszélések tényleges kihasználását.

Az egyszerűbb rendszerek gazdaságilag kedvezőbbek rövid és középtávon, de hosszú távon nem feltétlenül támogatják az összetett fenyegetésszélést és hálózati integrációt. Éppen ezért a gazdasági mutatók – különösen a TCO és az NPV – rendszeres felülvizsgálata elengedhetetlen a stratégiai döntésekhez.

A kutatásom során arra a megállapításra jutottam, hogy a biztonságtechnikai rendszerek élettartama, elavulása és technológiai fejlődése szoros kölcsönhatásban állnak egymással. A fizikai élettartam ugyan továbbra is meghatározó, de a technológiai elavulás – különösen a digitális, hálózatra kapcsolt eszközök esetében – gyakran hamarabb indokolja a cserét, mint a műszaki meghibásodás. Ez a felismerés fontos hatással van arra, hogyan kell tervezni és üzemeltetni egy korszerű biztonságtechnikai rendszert.

A különböző eszköztípusok élettartama jelentősen eltér, különösen a szoftveresen komplex rendszerek esetében, ahol az erkölcsi elavulás gyakran 4–6 éven belül bekövetkezik. A gazdasági megtérülés nem csupán a beruházási költségektől függ, hanem szorosan kapcsolódik az üzemeltetési költségekhez, a karbantartási igényekhez és a rendszer funkcionalitásához. A TCO és ROI mutatók összehangolt alkalmazásával hosszú távon fenntartható és hatékony beruházási döntések hozhatók. Az új technológiák bevezetése akkor éri meg, ha az adott védelmi célrendszer képes kihasználni az általuk nyújtott előnyöket, például az AI-alapú elemzéseket vagy a hálózati integrációt.

KONKLÚZIÓ

A kutatás tapasztalatai alapján több gyakorlati javaslatot fogalmazok meg.

Először is, érdemes életciklus-szemléletű tervezést alkalmazni, amely már a biztonságtechnikai rendszerek kiválasztásának a fázisában figyelembe veszi a várható élettartamot, a technológiai fejlődést és a gyártói támogatási időszakot.

Másodszor, a rendszeres TCO és ROI elemzések támogatják az eszközök állapotának és költséghatékonyságának időszakos értékelését, különösen nagyobb léptékű infrastruktúrák esetében, így elősegítve a tudatos döntéshozatalt.

Harmadszor, a gyorsan elavuló technológiák kezelésére célszerű 3–5 éves frissítési ciklust bevezetni, amely lehetővé teszi a fokozatos fejlesztést a teljes rendszer lecserélése nélkül.

Negyedszer, előtérbe kell helyezni az integrációs képességeket, olyan rendszereket választva, amelyek könnyen összekapcsolhatók más alrendszerekkel, például tűzjelző vagy épületfelügyeleti rendszerekkel, ezzel növelve az adatáramlás és a döntéstámogatás hatékonyságát.

Végül, a modern technológiák alkalmazása megköveteli a kezelőszemélyzet rendszeres képzését és a gyártói vagy szolgáltatói támogatás aktív igénybevételét.

Ezek a javaslatok hozzájárulnak ahhoz, hogy a biztonságtechnikai beruházások hosszú távon fenntarthatók, költséghatékonyak és technológiailag korszerűek maradjanak. A tudatos döntéselőkészítés és az életciklus-alapú szemlélet nemcsak a költségvetés hatékonyságát növeli, hanem a védelmi szint fenntartását is biztosítja.

FELHASZNÁLT IRODALOM

- [1] Enisa, „Security of Industrial Control Systems,” European Union Agency for Cybersecurity, online, 2020.
- [2] B. T. Bognár Balázs, KRITIKUS INFRASTRUKTÚRÁK VÉDELME I., Budapest: Dialóg Campus Kiadó, 2019.
- [3] Keenfinity-group, „Product Life Cycle Planning Guide,” 2022. [Online]. Available: <https://www.boschsecurity.com/xe/en/support/product-security/>.
- [4] „IEC 62820-1:2016: Video surveillance systems for use in security applications – General requirements,” 2016.
- [5] Z. Zsolt, „A biztonság és abiztonságmenedzsment vizsgálata vállalati nézőpontból,” Hadmérnök, %1. kötet15, %1. szám1, pp. 19-29, 2020.
- [6] Security Science: The Theory and Practice of Security, Butterworth-Heinemann, 2013.
- [7] Isaac Kohen, „How to calculate your return on security investments,” online, 2019.
- [8] T. L. Néma Szabolcs, „Gazdasági optimalizáció az objektumvédelemben,” Magyar Rendészet, %1. kötet24, %1. szám4, p. 121–144, 2024.
- [9] R. Naegle, „Strategic IT Cost Optimization That Goes Beyond Slashing Spend,” gartner, online, 2025.
- [10] „A karbantartás szerepe a vagyonvédelmi rendszerek életciklusában,” 2021.
- [11] „UL 2800-1 Standard: Performance and Reliability of Security Equipment,” UL, 2021.
- [12] Koorsen Fire & Security, „How Important Is Regular Maintenance for Commercial Security Systems,” Koorsen Fire & Security, online, 2024.