ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Biztonságtudományi és Kibervédelmi Intézet

SZAKDOLGOZAT

OE-BGK

2025.

Hallgató neve: Márfi Tamás László [redacted]

Hallgató törzskönyvi száma: T012281/FI12904/B

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Óbudai Egyetem
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Biztonságtudományi és Kibervédelmi Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: Márfi Tamás László
Szakdolgozat száma: [redacted]
Törzskönyvi száma: T012281/FI12904/B **Neptun kódja:** [redacted]

Szak: biztonságtechnikai mérnöki
Specializáció: biztonságtechnikai mérnöki - biztonságtechnikai

A dolgozat címe: Egy fiktív épület objektumvédelme
A dolgozat címe angolul: Physical Security of a Fictional Facility
A feladat részletezése:
1. Az objektumvédelem elméleti alapjainak és szabályozási környezetének ismertetése.
2. A védendő létesítmény biztonsági szempontú elemzése és kockázatelemzése.
3. Fizikai védelmi rendszerek tervezése és integrációja technikai eszközökkel.
4. Élőerős őrzés szerepe és operatív működtetése az objektumvédelemben.
5. Komplex biztonsági rendszer működése és incidenskezelési protokollok.

Intézményi konzulens neve: Dr. Pető Richárd

A kiadott téma elévülési határideje: 2027. 12. 15.
Beadási határidő: 2025. 12. 15.

A szakdolgozat: Nem titkos.

Kiadva: Budapest, 2025. 10. 27. P.H. .....
Intézetigazgató

A dolgozatot beadásra alkalmasnak találom: 2025. 12. 15.

.....
belső konzulens

.....
külső konzulens

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Biztonságtudományi és Kibervédelmi Intézet

HALLGATÓI NYILATKOZAT

Alulírott **Márfi Tamás László** [redacted] hallgató kijelentem, hogy a szakdolgozat saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja, a titkosításra vonatkozó esetleges megkötések mellett.

Budapest, 2025. december 02.

Márfi Tamás László

.....

hallgató aláírása

eua

1081 Budapest,
Népszínház u. 8.

+36 (1) 666-5414
+36 (1) 666-5300

email@uni-obuda.hu
www.uni-obuda.hu

EGY FIKTÍV ÉPÜLET OBJEKTUMVÉDELME

TARTALOMJEGYZÉK

BEVEZETÉS

Magyarországon a rendszerváltást megelőző évtizedekben a tulajdontárgyak nagyrésze állami tulajdonban állt, ezért azok védelmét is az állam látta el. A politikai irányvonal megváltozásának köszönhetően azonban jelentős mértékben megnőtt a magántulajdon hányada, ezzel párhuzamosan az állampolgárok igénye tulajdonuk védelmére. A magántulajdonosok részére az állam védelmi kötelezettséget ugyan nem írt elő, hanem megalkotta annak jogszabályi feltételeit. Azáltal, hogy az addig meglévő és az újonnan kialakuló társadalmi csoportok között egyre nagyobb mértékben nőttek a vagyoni különbségek, országhatárok nyíltak meg és országhatárokon átívelő bűnszövetkezetek alakultak elsősorban vagyon elleni bűncselekmények elkövetésére és információlopásra, így megnőtt az igény a védelmi eszközök, rendszerek kialakítására és megszervezésére. Előbbiek okán az olyan szakterületek, mint a tűzvédelem, iparbiztonság, polgári védelem, stb. hozták magukkal a biztonságtechnikát, mint interdiszciplináris tudomány kialakulását, mely szűkebb értelemben a tulajdon és a személy védelmével foglalkozik, tágabb perspektívából ide sorolható a közlekedés-,repülés-, ipar-, energia- és atomenergia biztonság, információvédelem is. Következtetésképpen szorosan kapcsolódik számos műszaki tudományhoz, mint pl. építőmérnök, gépészmérnök, villamosmérnök, vegyészmérnök, katonai műszaki tudomány. [1] [2] [3]

A fentebb részletezett okokkal összefüggésben elkezdtek teret hódítani a komplex vagyonvédelmi rendszerek, vagyis a mechanikai- és élőerős védelem, elektronikai jelzőberendezések, illetve a szervezeti intézkedések egyidejű alkalmazása. Ezen rendszerek alkalmazása sem nyújt azonban teljes körű védelmet, de megfelelő alkalmazásuk esetén a maradék kockázatot képesek lehetnek minimalizálni. [1] [2]

A dolgozatom címének kiválasztásakor törekedtem arra, hogy olyan téma vizsgálatáról értekezzek, amivel átfogó és lakonikus képet tudok adni egy fiktív épület objektumvédelméről. A bemutatandó épület háromszázötven négyzetméter alapterületű földszinti irodaépület, melynek tulajdonosa a biztonságtechnikai-, elektronikai szórakoztató eszközök értékesítésével és részben szoftverfejlesztéssel foglalkozó FutureAi Kft. elnevezésű cég. Funkciója szerint irodaépület, melyben bemutató tér is

helyet kapott. A cég húsz fő munkavállalót foglalkoztat, akik munkatevékenysége kizárólag monitor előtti munkavégzést foglal magában. A dolgozók az őrszolgálattal rendelkező porta beléptetési pontján keresztül juthatnak be és foglalhatják el a munkaállomásaikat. Az objektumba való beköltözés folyamatban van, jelenleg az irodai bútorzat és munkaeszközök, épületgépészeti berendezések találhatóak meg, a komplex vagyonvédelmi rendszer kialakítás alatt áll. Utóbbi koncepció tervének elkészítésére kaptam előzetes megbízást a cég részéről.

Az első fejezetben az objektum fogalmát, alapjait és hazai jogszabályi környezetét mutatom be. Ezt követően a második fejezetben elemzem a kitalált létesítményt biztonsági szempontok szerint, valamint értékelem a felmerülő kockázatokat alapján készített kockázatelemzést. A dolgozat harmadik fejezetében a fizikai védelem és annak megvalósítása kerül fókuszba. A biztonságtechnikai eszköztípusok javaslatai során törekedtem a védelem leghatékonyabb kiépítését fókuszba helyezni.

A negyedik fejezetben bemutatom a megszervezendő élőerős őrzését, a vagyonőri szolgálatot. Részletezem annak szerepét és működését. Dolgozatom utolsó részében különbséget teszek a komplex és az integrált objektumvédelem között, valamint kitérek az incidenskezelési protokollra. Végezetül összegzem dolgozatom tartalmát és javaslatokat fogalmazok meg a jövő vagyon- és őrzésvédelmét véleményem szerint magasabb szintre emelő tényezőkkel kapcsolatban. Fontosnak tartom kiemelni, hogy tűzvédelmi vonatkozású kérdésekkel, berendezésekkel csak érintőlegesen foglalkozom és csak a saját szubjektív megítélésem szerinti, az objektum biztonsági szempontjából fontosabb tényezőket tárgyalom. A védelem ellátására javasolt biztonságtechnikai eszközök műszaki megfelelősségéről, technikai jellemzőiről, az azokhoz tartozó szabványok részletes elemzéséről jelen munkámban nem értekezem. A dolgozat szerkesztését 2025. december 1-jén zártam le, a feltüntetett források a zárás időpontjáig megtekinthetőek voltak.

1. AZ OBJEKTUMVÉDELEM ELMÉLETI ALAPJAI ÉS SZABÁLYOZÁSI KÖRNYEZETE

Hazánkban a biztonságtudomány és ezen belül a biztonságtechnika a huszadik század végén jelent meg. Számos igencsak eltérő, de mégis egymásba kapcsolódó szakág megjelenését és egyben fejlődését hozta magával, úgy mint a kórházbiztonság, repülőtéri utasbiztonság, kritikus infrastruktúra- és veszélyes anyagokkal foglalkozó üzemek védelme, tűzvédelem vagy éppen a személy- és vagyonvédelem. Utóbbin belül meghatározó az őrzés-védelem, objektumvédelem vagy más néven objektumbiztonság. Fontos megjegyezni, hogy a szakterületen belüli fogalmakat, alapelveket a rendelkezésre álló szakirodalmi források a mai napig különféleképpen értelmezik az adott területre fókuszálva. Ezért először azok áttekintése és pontos meghatározása szükséges. [4]

1.1. Az őrzés

Az őrzés-védelem vagy másképpen őrzés és védelem egymás követő tevékenységek sorozata. A kettő közötti határvonal nagyon vékony, mégis lényeges különbség van közöttük.

Fogalmát tekintve az őrzés egy olyan a védelmet megelőző irányított és szabályozott rendben végrehajtott ellentevékenység, melynek során egy adott személy vagy csoport esetlegesen bekövetkező szándékos vagy vétlen jogellenes tevékenységét akadályozza meg a védendő területre való bejutást és az onnan való eltulajdonítást meggátolva, illetve azt jelentős mértékben lelassítva. A tevékenység maga egy feladat, amit jogszabályok, céges belső szabályozók (például vagyonvédelmi szabályzat) vagy utasítások által meghatározott keretek között kell végrehajtani. Az őrzési tevékenység optimális esetben hosszabb ideig, akár évekig is eltarthat egészen az előre nem várt incidens bekövetkeztéig. A feladatot a szolgálatban lévő személy (őr) vagy személyek (őrség) látják el. A vagyonbiztonsági szempontból védendő tulajdon megjelenthet statikus-, mozgó-, valamint kevésbé és kiemelten veszélyeztetett állapotban is. Ezen jellemzők alapján a személy- és vagyonvédelem főbb területei az objektumbiztonság, a speciális vagy kritikus objektumok biztonsága, pénz- és értékszállítás, szállítmánykísérés,

rendezvénybiztosítás. Az őrzésvédelmet ellátó személyek munkájának hatékonyságát növeli a pontos, megfelelő szolgálatszervezés és a védett objektumtól függően szolgálati fegyver rendszeresítése, őrkutya alkalmazása, valamint biztonságtechnikai eszközök üzemeltetése, mint például beléptető- és CCTV kamerarendszer, kártyajogosultságok szabályozása, kulcstároló széf, informatikai rendszerek és mindezek kombinációja. Lényeges külön megemlíteni, hogy amennyiben az őrzés egy adott személyre vonatkozik, úgy azt már személybiztosításnak vagy személyvédelemnek nevezzük. A biztosítás alatt védett vagy kiemelten védett személyek értendőek, mint például magas pozíciójú hivatali tisztviselők, miniszterek, kormányfők, elnökök. Napjainkra már a magánbiztonsági szolgáltatást nyújtó cégek széles választéka érhető el a piacon, ezáltal a vagyonosabb celebek, sportolók, üzletemberek is igényt tartanak biztonsági személyzetre. [4] [5]

Összefoglalva az őrzés célja tehát a biztonság megteremtése és fenntartása az élőerős védelemmel, illetve a rendelkezésre álló biztonságtechnikai eszközökkel. A hatékony őrzés, valamint a megfelelően kiépített és már az objektumon kívülről is szembetűnő vagyonvédelmi rendszer az esetek többségében biztosít akkora visszatartó erőt, hogy a büntetendő behatolási kísérlettől eltántorítja a potenciális elkövetőt. [2] [5]

1.2. A védelem

A védelem szoros kapcsolatban áll az őrzéssel és általánosságban elmondható, hogy az azt követő ellentevékenység, melyet az őrzési feladattal megbízott személy vagy személyek hajtanak végre szabályozott módon és a tevékenységüket a rendelkezésre álló vagyonvédelmi eszközök támogatják meg. Lexikálisabb értelmezése szerint az egyén általi döntésen alapuló cselekvés, folyamat, amely a jogellenes magatartás vagy tevékenység megszüntetésére, megakadályozására irányul annak érdekében, hogy az esetlegesen bekövetkező negatív következményeket mérsékelje vagy teljes egészében elhárítsa. [5]

Az őrzés során folyamatos a készültségi állapot, azonban nem tudjuk, hogy az incidens mikor, hol, ki által és hogyan fog bekövetkezni, illetve milyen arányú ellentevékenységet kell alkalmaznunk. A nem várt esemény bekövetkezésekor előbbi kérdések tisztázódnak

és ha az elkövető tovább folytatja a megkezdett cselekvését (például egy telephelyre való jogosulatlan belépést), akkor életbe lép ezen ellentevékenység. [4]

A védelem csak akkor tud aktiválódni, ha előtte az adott objektumot megfelelően elemezték, kockázatbecslést készítettek, majd ezek alapján szervezték meg a mechanikai védelmet, őrzésvédelmet, elektronikus jelzőrendszereket. A létesítendő berendezések tervezésekor külön figyelmet kell fordítani a külső és belső védelem kialakítására. Ennek részleteit a dolgozatom későbbi szakaszában fogom ismertetni. [4]

Az előre telepített védelmi eszközök nyújtotta biztonságon kívül meg kell említeni, hogy a védelem rendelkezik egy sajátos formával is. Ebben az esetben személyeket, különböző természeti területeket vagy műemlékeket is védelem alá helyezhetünk. A valóságban ez úgy néz ki, hogy a jogalkotó az érintett objektum specifikus jellemzőit figyelembe vevő jogszabály kidolgozásával, majd annak az Országgyűlés általi elfogadását követő hatályba lépéssel nyújt passzív oltalmat a szükséges „objektum” részére. A mindennapi életünk során számos alkalommal találkozunk jogilag védett dolgokkal. Ilyenek lehetnek az erdők, nemzeti parkok, műemléki épületek, közterületi szobrok, egyházi épületek vagy a kritikus infrastruktúra szempontjai alapján a bankok, kórházak, távközlési és közművek szolgáltatási létesítményei. Tökéletes példa erre vonatkozóan a hazánkban foganatosított intézkedések sorozata árvízi helyzetkor. A patakok mentén ugyan a vízügyi szakemberek előre meghatározott rendszerességgel bejárásokat tartanak azok meder és rézsű állapotának szemrevételezésére annak érdekében, hogy a víz szabad lefolyását gátló esetlegesen akadályozó tényezők (növényi és egyéb eredetű felhalmozódott hordalék) eltávolításra kerüljenek. Azonban ezen tevékenység például a Duna és a Tisza mentén kevésbé hatékony azok mérete okán. A hatályos jogszabályok, valamint a meteorológiai előrejelzés és vízhozam figyelő rendszerek alapján az előre telepített vízmércék adott szintjének víz általi elérése esetén aktiválásra kerül az árvízvédelmi intézkedési protokoll. Megalakulnak a védelmi bizottságok, az árvízvédelmi operatív törzs és az elöntéssel veszélyeztetett településeken és folyószakaszokon megkezdődik a védekezés homokzsákokkal, mobil- és tömlősgátakkal, szivattyúkkal, stb. Az erdők és kirándulóhelyek esetében is hasonló helyzet áll fenn, ugyanis azok épségét jogszabályok által védik, úgymint hulladékgyűjtő edények kihelyezése, dohányzás és tűzrakás tiltása.

Egy esetlegesen bekövetkező tűzeset alkalmával a védelemben vagy védekezésben érintett elsőszámú beavatkozó erők a tűzoltók lesznek, akik vízsugarakkal vagy szélsőséges esetben ellentűz gyújtásával megpróbálják a további károkat minimalizálni. A műemlék jellegű objektumok is a jog általi védelem alatt állnak és csak jogellenes tevékenység (például rongálást) követően lépnek életbe a védelmi intézkedések. [4] [5]

Fentieket összegezve elmondható, hogy a védelem komplexebb tervezést igényel, mint az őrzés, illetve az adott incidensre adott intézkedések csak abban az esetben lesznek hatékonyak ha azok az előre meghatározottak szerint, rutinszerűen és hiba nélkül kerülnek végrehajtásra. A tevékenység megszervezése lényegében kettő alapelven nyugszik. Egyrészt az objektum kockázatelemzésen alapul, melyből következik a második elv, vagyis a biztonsági szerkezet kialakítása. Az elemzés során minden részletre kiterjedően fel kell mérni a védett dolog tulajdonságait, jellemzőit, vagyis az anyaghasználatot, a működését, értékét, közvetlen és tágabb környezetét, veszélyforrásokat. Az elkészült kockázatelemzés alapján meg kell határozni az optimális és arányos védelem kialakítását a várható legnagyobb veszély eredményes elhárításához szükséges élőerő és technikai eszközök vonatkozásában. [2] [4] [5]

1.3. Az objektum

Az őrzés és a védelem fogalmának tisztázása után szükséges a személy- és vagyonvédelem egyik főbb területének, vagyis az objektumvédelem központi tárgyát képező objektumot részletezni.

Az objektum szó latin eredetű és tárgyat, építményt jelent. Az elmúlt évezredek alatt a társadalom, építészet, gazdaság, technológia folyamatos fejlődésével és a vagyoni elemek felhalmozásával azonban ma már sokféleképpen értelmezhetjük. A különböző tudományok általi meghatározásoknak sok közös és eltérő nézőpontjuk is van. Nem mindegy, hogy katonai, rendészeti, térképészeti, természeti, IT (Information Technology, magyarul Infomációs Technológia), IoT (Internet of Things, magyarul a dolgok internete), gazdasági, vállalat- vagy magánbiztonsági szempontból használjuk a kifejezést, ugyanis ezen szakágak különböző tárgyat, területet, információt, adatot vagy

személyt értenek az objektum alatt. Előbbiek okán beszélhetünk lőszerraktárról vagy vezetési pontról, a térkép által ábrázolt erdőről, egy népszerű nemzeti parkról, számítógépeken az információk tárolásáról, okosotthonok egymásba integrált rendszereiről, pénzügyi adatokról és azok elemzéséről vagy jelen dolgozat témájaként választott fiktív épületről. A legfőbb közös pont az eltérő meghatározások között a védelem szükségessége és ez a két szó adja meg a fogalom részbeni lényegét is: az adott tárgy, szobor, információ, stb. objektummá minősülésének feltétele, hogy azt előzetesen a döntés meghozatalára jogosultsággal rendelkező személy őrzendővé és védendővé nyilvánítsa. Az objektum tehát olyan létesítmény vagy dolog, melynek őrzésvédelmét személy, jogszabály vagy egyéb rendelkezés írja elő. A védelem célja az objektum működésének-, integritásának-, valamint az élet- és vagyonvédelemnek a biztosítása. [4] [5]

A fogalom meghatározás alapján egyértelműen kijelenthető az objektum komplexitása, mely véleményem szerint már a közeli jövőben további értelmezéseket fog kapni a tudományok, de legfőképpen a mesterséges intelligencia fejlődésével és a hétköznapi életbe való beintegrálásával.

1.4. Az objektumvédelem

Az őrzés és védelem, valamint az objektum elméleti alapjainak tisztázása után az objektumvédelemről, mint a személy- és vagyonbiztonság egyik meghatározó részegységéről adok áttekintést.

A védelem hatékony megtervezésének és kialakításának elengedhetetlen részét képezik az előzetes vizsgálatok lefolytatása, vagyis a biztonságot esetlegesen veszélyeztethető elemek, tulajdonságok, jellegzetességek vizsgálata, valamint az objektumban végzett munkatípusok meghatározása. Előbbiek alapján a létesítményt többféle módon lehet csoportosítani, melyek közül kettőt emelnék ki. Az első a funkció szerint történik, így megkülönböztetünk köz- és magánépületeket, közösségi- és ipari létesítményeket, speciális objektumokat és kritikus infrastruktúrákat. A második a befolyásolási tényezők

szerinti csoportosítás, azaz figyelembe vesszük az elhelyezkedést, az ahhoz kapcsolódó kockázatokat. [6]

Hazánkban egészen a rendszerváltozásig az objektumok védelme nagy részben az élőerős őrzésre és a mechanikai-fizikai védelemre korlátozódott. A technológia fejlődésével megjelentek a kezdetleges elektronikai jelzőrendszerek, vagyis a különböző riasztók, CCTV rendszerek, behatolás- és nyitásjelzők. Fontos megjegyezni, hogy ezen eszközök nem adnak valós védelmet, mivel például a telephelyre jogosulatlanul belépő személyt vagy gépjárművet nem tartóztatják fel, csak jelzést adnak le az őrszolgálat felé annak tényéről, illetve rögzítik és naplózzák az eseményt. A detektálást követően a további intézkedések megtétele az élőerős védelem feladata. Az integrált áramkörök (IC, vagyis Integrated Circuit) megjelenésével az érzékelési technológiák rohamos fejlődésnek indultak, aminek köszönhetően a megfelelően tervezett és kivitelezett rendszerek rendkívül észlelési érzékenységűek lettek, továbbá képesek már egymással és az élőerővel is szoftveres módon kommunikálni. [3]

A fejlődés új ipari ágazatokat is létrehozott és ezzel egyidejűleg a támadóknak új támadásifelületeket és eszközöket adott a kezébe. Egyre több és egyre nagyobb globális multinacionális cég alakult, melyek hatalmas tudásanyagot, innovációt és szenzitív információt halmoztak fel. Ezeknek a védelme kiemelt fontosságú a „multik” számára, de a korábbi klasszikus mechanikai-fizikai védelmi megoldások nem tudják megakadályozni a kiber jellegű bűncselekményeket. Ezért a biztonságtechnikán belül megjelent egy új részterület is, vagyis a kibervédelem, amit a piaci szereplőkön kívül az államhatalom is alkalmaz, illetve a magánszemélyek felhasználási oldalán is nagyobb hangsúlyt kap az adatok védelme, mint például erős jelszó (8-12 karakter, kis- és nagybetű, speciális karakter) beállítása vagy a kétfaktoros hitelesítés (e-mail, sms, biometrikus azonosítás). [3]

Tekintettel arra vonatkozóan, hogy napjainkban a kibervédelem, mint új tudományág rohamosan fejlődik és már elengedhetetlenül az objektumbiztonság részét képezi, így a korábbi definiálást kiegészítendő az objektumvédelem olyan jogi védelmi- és azon belül mechanikai eszközök, elektronikai jelző- és IT rendszerek, szervezeti szabályozók

egységbe foglalása, melyek felügyeletét élőerő és megfelelő képesítéssel rendelkező szakemberek látják el. A létrehozott védelem célja az objektum fizikai- és elektronikus információs integritásának megőrzése, továbbá a bekövetkező incidensek okozta károk megelőzése vagy minimalizálása. Ezek alapján az objektumbiztonság elemeit képezik a jogi védelmi-. mechanikai-, technikai eszközök, az élőerős őrzés, a kialakított intézkedési rendszer, valamint a szakértői felügyelet. Egységes védelemként való alkalmazásuk esetén komplex vagyonvédelemről, illetve közös kommunikációs hálózatba kapcsolásukkal integrált rendszerről beszélhetünk. [3] [5]

1.4.1. A mechanikai védelem

Primer védelemnek minősül azon oknál fogva, mivel a támadó először ezzel szembesül, mint leküzdendő akadály, melyet további három részre bonthatunk.

A kültéri mechanikai védelmet első vonalát általában a védendő objektum környezetébe célszerű kivitelezni, mivel az előre nem kitervelt behatolási kísérlet ellen erős preventív üzenetet hordoz magában. Ilyenek lehetnek az árkok, töltések, (biztonsági) kerítések, kapuk, sorompók. Utóbbiakat kiegészítendően fontos megemlíteni a periméter védelmet is. Lényegét tekintve a külső mechanikai védelem megtámogatását jelenti elektrotechnikai eszközök telepítésével, mely által a támadás korai detektálása valósulhat meg. Ilyen eszközök lehetnek a rezgés- és mozgásérzékelők vagy a zártláncú videómegfigyelő kamerák. [4] [7] [8]

A héjszerkezet következő részegysége alatt az objektum szerkezeti elemeit és nyílászáróit értjük, úgy mint falazat, födém, ablakok és ajtók. Ezeket nagyon fontos már az épület tervezési fázisában körültekintően megvizsgálni, majd kivitelezni (például megfelelő fal- és födém vastagság, illetve szilárdság), mivel a későbbi módosítás jelentős költségekbe kerülne. Az ajtókból és ablakokból szintén érdemes megfelelő minőségű biztonsági változatot választani, továbbá szükség esetén azokon a MABISZ (Magyar Biztosítók Szövetsége) ajánlásainak megfelelő rácsot és jó minőségű zárszerkezetet alkalmazni. Az objektumba belépni szándékozó személyek jogosultságának kezelése szempontjából szükség esetén beléptető kapuk alkalmazása célszerű. Figyelembe véve a Belügyminisztérium által minden évben közzétett bűnügyi statisztikákat általánosságban

elmondható, hogy a betörés jellegű bűncselekmények döntő részét a nyílászárókon keresztül valósíthatják meg. Ennek köszönhetően a piac is reagált és biztonsági megoldások széles választékát kínálja megvásárlásra, mint például több ponton záródó zárszerkezetek, reteszelhető kilincsek, lakatok, üvegfelületekre applikálható biztonsági fóliák. A kialakítandó mechanikai-elektronikai eszközök együttesen a telekhatármenti és az épület szerkezeti elemei közötti védelmét tekintve periméter távolságot hoznak létre. [4] [7] [9] [10]

Az utolsó részegység a mechanikai tárgyvédelem, mely jórészt a pénzügyi intézeteknél, múzeumoknál, érték- vagy pénzszállításnál kerülhet előtérbe. Ezeknél az eseteknél a védendő objektum lehet egy kiállított műtárgy, amit többrétegű biztonsági üveggel védenek. Az üveg fajtája szerint lehet törés álló (fizikai behatást követően az üvegrétegek közötti speciális fólia miatt az üvegdarabok nem szóródnak szét, ezáltal nem keletkezik nagyobb rés a felületen) vagy akár lövedékálló is. [4] [7]

Ezen technológia hatékonyságát korábbi munkatapasztalatom során személyesen is megtapasztaltam. A példának hozott duplarétegű biztonsági üvegtábla két telephelyet összekötő híd gyalogos folyósóját határolja és egyben gátolja meg az onnan történő kiesést. A táblán nagy erejű fizikai impulzust követően (KCR gépjármű behúzatlan gémjének köszönhetően) repedések keletkeztek, azonban az a tartósínjeiből nem csúszott ki, ellenben cseréje szükségessé vált. A tűzoltóság által műszaki mentés során kézi szerszámgépekkel az üveg elfűrészelésre került, majd körülbelül 6 méter magasból az útpályára zuhant. Az esés következtében az üvegtábla ugyan ketté hajlott a közel ötszáz kilogramm tömege miatt, de a felület egyben maradt, minimális szilánk kiszóródástól eltekintve. A tábla állapotát a 1. ábra mutatja.

1. ábra: Az üvegtábla lezuhanást követő állapota [Saját kép]

A tárgyvédelmi eszközök lehetnek továbbá széfek, páncélszekrények vagy érték- és pénzszállító táskák. ‚kivitelüket tekintve lehetnek tűzállóak és betörésbiztosak, illetve a kettő kombinálásából kialakított értéktárolók. Ki kell emelni, hogy ezen eszközök is csupán késleltetni tudják a támadót célja elérésében, hiszen feltörhetetlen eszköz még nem létezik. [4] [7]

1.4.2. Az elektronikai jelzőrendszer

Az objektumvédelem hatékonyságát az elektronikus védelmi eszközök alkalmazásával növelhetjük meg. Fontos leszögezni azonban, hogy ezen rendszerek nem nyújtanak valós fizikai védelmet. Jelentőségük abban rejlik, hogy az épületbe való illetéktelen bejutást, a védett tárgyak, értékek, információk eltulajdonítását vagy a védelem alatt álló személy elleni támadást jelzik a beavatkozó élőerőnek. Hatékony rendszert képezve a mechanikai védelem mindaddig megakadályozza és visszatartja az elkövetőt, ameddig a jelzőrendszer nem riasztja az őrszolgálatot, akik végrehajtják a további szükséges intézkedéseket az incidens elhárítására vagy a károk minimalizálására. Általánosságban kijelenthető, hogy a megfelelően kiépített mechanikai és elektronikus védelem már önmagában is visszatartót erőt képes felmutatni. Elég csak a szociális médiában terjedő videóanyagokra gondolni, melyben az elkövető kerítés leküzdés, gépjármű feltörés vagy egy könnyűnek ígérkező pénztárca lopás közben fedezi fel a térfigyelő kamerát, majd tervével gyorsan felhagyva próbál meg a kamera látóteréből eltűnni. [2] [4] [6] [7]

A jelzőrendszerek telepítésével héjvédelmen belül további rétegeket alakíthatunk ki, melyek a következő lehetnek: kültéri-, felület-, tér-, tárgy- és személyvédelem. Előbbieket további kategóriákra bonthatjuk az eszközök funkciója szerint:

- Zártláncú videómegfigyelő rendszerek (például cső-, kompakt-, ipari- és Dome kamerák, videófelvevő egység és analitika).
- Beléptetési rendszerek (kártyaolvasók).
- Ajtó- és kapunyitó rendszerek (normál vagy fordított működésű zárszerkezet, kulcsos- és kártyaolvasós ajtók).
- Behatolás jelző rendszerek (mozgás- és nyitásérzékelők).
- Távfelügyeleti rendszerek (a behatolás jelző rendszereket ellenőrzi és szükség esetén átjelzéssel riasztja a beavatkozó erőket, felügyeletet).
- Őrszolgálat ellenőrző rendszerek (járőrözési útvonalon elhelyezett ellenőrző pontok).
- Személy- és csomagátvizsgáló rendszerek (áruvédelmi kapuk).
- Tűzjelző rendszerek (tűzjelző központok, láng- vagy füstérzékelők, kiürítést számláló rendszerek).

A védelmi eszközökből az előbbi felsoroláson kívül jóval szélesebb választék érhető el a piacon. A jelzőrendszereket más szempontok alapján is csoportosíthatjuk, mint például felhasználási területek, műszaki jellemzőik, kialakításuk és az alkalmazott technológiájuk alapján, aminek bemutatása jelen dolgozatomnak nem képezi tárgyát. [4] [6] [7]

1.4.3. Az élőerő

Az informatika, azon belül is a digitalizáció, mesterséges intelligencia, robottechnológia, hardver és szoftver fejlődéssel napjainkban már a jelzőrendszerek széles választéka érhető el, ami egyben mind inkább háttérbe kezdi szorítani az élőerő szerepét. Azonban azok a cégek, melyek kisebb pénzügyi forrásból tervezik a védelmi kialakításukat vagy szaktudás hiányában nem ismerik a biztonságtechnikai eszközöket, illetve azok szerepét lebecsülik a hatékony védekezésben még mindig kizárólag vagyonőröket alkalmaznak. Az őrség tervezése, megszervezése és irányítása összetett folyamat eredményeként jön létre és szintén elengedhetetlen részét képezi a komplex védelemnek, melyről részletesebben a 4. fejezetben értekezem.

1.5. Az objektumvédelem szabályozása

Munkatapasztalatom során eltérő véleményekkel találkoztam azt illetően, hogy az adott objektum védelmének kialakítására milyen igény mutatkozik megrendelői oldalról. Az egyik nézőpont szerint kivétel nélkül a jogszabályok által meghatározott minimum követelményeknek való megfelelés a célkitűzés, más álláspont alapján akár nagyobb anyagi ráfordítás a jellemző. Az én megítélésem szerint a megrendelői igények egy összetett folyamat eredményeként alakulnak ki és magánszemélyenként, illetve cégenként változnak. Következésképpen a kisebb méretű cégeknél, vidéki közigazgatási intézményeknél ugyan rendelkezésre állhat a védelem tervezéséhez szükséges szakértelem, de forráshiány okán nem telepítenek jobb minőségű CCTV kamera- vagy beléptető rendszert. Ugyanakkor előbbi ellentétje is előfordulhat, vagyis egy nagyobb vállalatnál a védelem költségvonzata nem terheli meg az éves büdzsét, de szaktudás hiányában nem vagy nem megfelelően épül ki a biztonsági rendszer.

A hazai jogszabályi környezet törvényekből, rendeletekből, utasításokból, intézkedésekből, ajánlásokból áll, melyek különböző rendvédelmi hatóságokhoz, államhatalmi intézményekhez, létesítményekhez, tevékenységekhez kötődnek, valamint a biztonságtechnikával kapcsolatban számos tudományágra és szakterületre tagozódnak szét. [1] [11]

A következő felsorolásban a megítélésem szerinti legfontosabbakat említem meg:

- *„A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól*” szóló 2005. évi CXXXIII. törvény [12]
- *„A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény végrehajtásáról”* szóló 22/2006. (IV.25.) BM rendelet [13]
- *„A Rendőrségről” s*zóló 1994. évi XXXIV. törvény [14]
- *„A fegyveres biztonsági őrség Működési és Szolgálati Szabályzatának kiadásáról”* szóló 27/1998. (VI.10.) BM rendelet [15]
- *„A honvédelemről és a Magyar Honvédségről”* szóló 2021. évi CXL. törvény [16]

- *„A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról”* szóló 2011. évi CXXVIII. törvény [17]
- *„Az Országos Tűzvédelmi Szabályzatról*” szóló 54/2014. (XII.5.) BM rendelet [18]
- Tűzvédelmi Műszaki Irányelvek [19]
- *„A kritikus szervezetek ellenálló képességéről”* szóló 2024. évi LXXXIV. törvény [20]
- *„A munkahelyen alkalmazott elektronikus megfigyelőrendszer alapvető követelményeiről”* szóló NAIH ajánlás [21]
- Magyar Biztosítók Szövetsége Vagyonvédelmi és Kármegelőzési Bizottság (MABISZ VKB) Betöréses lopás- és rablásbiztosítás technikai feltételei (ajánlás) [9]
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/697 RENDELETE *„a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)”* [22]
- *„Az információs önrendelkezési jogról és az információszabadságról”* szóló 2011. évi CXII. törvény [23]

A jogszabályokat követően fontos megemlíteni a vonatkozó szabványokat, melyek részben angol és egyéb idegen nyelveken érhetőek el, ezért értelmezésük a megfelelő szakmai nyelvtudás nélkül nehézkessé válik. Megértésüket és alkalmazásukat tovább bonyolítja, hogy általában csak termékszabványokról van szó, amik az egyes rendszerek alegységeivel foglalkoznak. A biztonságtechnikán belül egyedüliként a tűzvédelmi szabványok állnak rendelkezésre megfelelő tartalommal és nyelvi fordítással, mely dolgozatomnak nem képezik tárgyát. Az alábbi szűkös számú felsorolás az érvényben lévő és magyar nyelven is elérhető fontosabb objektumvédelmi szabványokat tartalmazza:

- MSZ EN 50131-1:2011, MSZ CLC/TS 50131-7:2010 szabványok, melyek a riasztórendszerekkel, behatolás- és támadásjelző rendszerekkel kapcsolatos [11] [24]
- MSZ EN 50134-1:2022, MSZ CLC/TS 50134-7:2006 szabványok, melyek a riasztórendszerekkel és segélyhívó rendszerekkel kapcsolatos [11] [24]
- MSZ CLC/TS 50136-4:2008, MSZ CLC/TS 50136-7:2007 szabványok, melyek a riasztórendszerekkel és riasztásátviteli rendszerekkel és berendezésekkel kapcsolatos [11] [24]

A digitalizáció következtében folyamatosan növekvő mennyiségű tárolt adat biztonságáról kell gondoskodni. Az utóbbi években elterjedt otthonról történő munkavégzés (angolul home office) során a digitális térbe (felhő-alapú tárolás) feltöltött információkkal szembeni, rohamosan fejlődő adatlopási technikákkal kapcsolatos biztonsági események kockázatának minimalizálása kulcsfontosságúvá vált. Ennek érdekében a biztonságtudományon belül megjelent és prominens részegységet töltött be a kibervédelem, mint az adat- és információbiztonság biztosításának és fenntartásának szakterülete. Számos szabvány és ajánlás került kidolgozásra, melyek közül magyar vonatkozásban a fontosabbakat említem meg:

- MSZ ISO/IEC 27001:2023 szabvány, mely az információ- és kiberbiztonsággal-, infomációbiztonsággal- és irányítási rendszerekkel kapcsolatos [25] [26]
- ISO/IEC 27002:2002 szabvány, mely gyakorlati útmutatást ad fenti szabvány tartalmának megfelelő végrehajtására [27] [28]
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2022. december 14-i (EU) 2022/2555 IRÁNYELVE *„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)”* [29] [30] [31]

Az előbbi felsoroltáson kívül számos szakterület rendelkezik irányadó idegen nyelven elérhető szabványokkal, melyek a tervezők és üzemeltetők munkáját hivatottak segíteni. Ezeknek mielőbbi magyar nyelvre történő átültetése és elmélyítése szükséges a hazai védelmi szektor hatékonyságának növelése érdekében.

Jelen fejezetben áttekintést adtam az objektumvédelem elméleti alapjairól és jogszabályi szabályozásáról. Kitértem az őrzés és a védelem, valamint az objektum fogalomkörére. Bemutattam az objektumbiztonság komplexitását, részegységeit és a hazai jogszabályokat, magyar nyelven elérhető szabványokat. A következő fejezetben ismertetem dolgozatom címének tárgyát, vagyis egy fiktív épület jellemzőit, majd elemzem annak fizikai biztonságát, végül a kockázatértékelési módszert, szempontokat fejtem ki bővebben.

2. A VÉDENDŐ LÉTESÍTMÉNY BIZTONSÁGI SZEMPONTÚ ELEMZÉSE ÉS KOCKÁZATELEMZÉSE

A sikeres, pénzügyileg is jövedelmező vállalkozás kialakításhoz és működtetéséhez elengedhetetlen az adekvát biztonsági szempontú elemzés, vagyis az épületet minden aspektusból figyelembe vevő kockázatazonosítása, kockázatelemzése, kockázatkezelése (vagy az angol Risk Management szavakból fordított kockázatmenedzsment) és a kockázat monitoring. Előbbi folyamatok a jól működő vállalatirányítási rendszer alapját képezik. Minőségében és mennyiségében (, vagyis az adott szakterületenkénti elkészítése és alkalmazása) főként külföldi nagyobb méretű vállalatoknál jellemző, de hazai környezetben is találunk számos példát (autóipar és azok beszállítói, pénzintézetek, gyógyszer- vagy építőipar). Forráskutatásom során tapasztaltam, hogy a biztonságtechnika tudományág fejlettsége és kutatása, valamint ehhez kapcsolódóan az ún. komplex vállalati biztonságmenedzsment leginkább az Egyesült Amerikai Államokban képviseli a legmagasabb szintet. Az új technológiák, innovációk, szemléletek és szabványok részben innen kerülnek át és integrálódnak be az európai rendszerekbe. [32] [33] [34]

Az értékelés és elemzés elkészítéshez komoly szakmai tapasztalatra, széleskörű tájékozottságra és logikus gondolkodásra van szüksége a tervezési jogosultsággal rendelkező biztonságtechnikai mérnöknek, valamint a kidolgozásban segédkező további szakterületeket képviselő személyeknek, mint például munkavédelmi-, tűzvédelmi-, gépész- vagy folyamatmérnöknek. A sor nem teljes, hiszen a biztonságtudomány, mint interdiszciplináris tudományág is számos másik szakterületre kapcsolódik rá. A kockázatelemzés megjelenik és fontos részét képezi a minőségirányításnak, munkavédelmi-, gépész-, épületgépész-, villamos, informatikai-, kiberbiztonsági területeknek, katasztrófavédelemnek, rendészettudománynak és például a pszichológiának is. Fontos megemlíteni az MSZ ISO 31000:2018 Kockázatmenedzsment. Irányelvek elnevezésű szabványt, mely magyar nyelven is elérhető már. A szabvány nem kötődik konkrét szakterülethez, ellenben általános metódust kínál a kockázatokkal kapcsolatos folyamatok vizsgálatára, ezért felhasználható

bármely cég esetében. A kockázatelemzés elkészítésére több módszer és megközelítés is létezik. Leggyakrabban a minőségi, vagyis kvalitatív és a mennyiségi, vagyis kvantitatív típusokat szokták alkalmazni. Előbbi pénzügyi adatokat mellőzve a biztonsági események hatását és valószínűségét értékelik és sorolják be kockázati kategóriákba. A kvantitatív módszer esetén rendelkezésre állnak konkrét költségvetési adatbázisok, melyek során a bekövetkező incidens által okozott kár mértékét akár hosszabb időtávlatban is meg tudják határozni az érintett entitásra levetítve. Ezen kívül létezik még a semi-kvalitatív elemzés, ami előbbi kettő kombinálását jelenti, pontosabban a részletesebb elemzés során a meghatározott paraméterek alapján pontszámokkal osztályoz. [32] [33] [35] [36]

A következő alfejezetekben bemutatom az épületet, annak környezetét, a különböző funkciójú helyiségeket. A kockázatazonosítás hatékony elkészítésének sarkalatos feltétele a védendő objektum és környezetének helyszíni bejárása, funkciójának megismerése, aminek során elvégezhető egyben az események bekövetkezési valószínűségének és hatásainak számításba vétele is, vagyis a kockázatelemzés. A kettő folyamatot véleményem szerint nem lehet élesen külön választani, ezért azokat egy alfejezetben vizsgálom meg. Ezt követően a kockázatértékelés során a kvalitatív módszert alkalmazom - mivel a cég információbiztonságra hivatkozva pénzügyi adatokat nem biztosított számomra - és elkészítem az objektum kockázati mátrixát. Azt elemzem és a harmadik fejezetben a kapott adatok alapján részletezem a kockázatkezelést, vagyis az incidensek megelőzésére és a károk minimalizálására javasolt védelmi eszközöket. A cégnek a kockázatmenedzsment részeként állásfoglalást kell kialakítani a fenyegetettségre, ami történhet a kockázatkerülés, kockázatcsökkentés, kockázatmegosztás vagy kockázatvállalás opciójával. [32] [33] [35]

2.1. A fiktív épület tulajdonságai, jellemzői

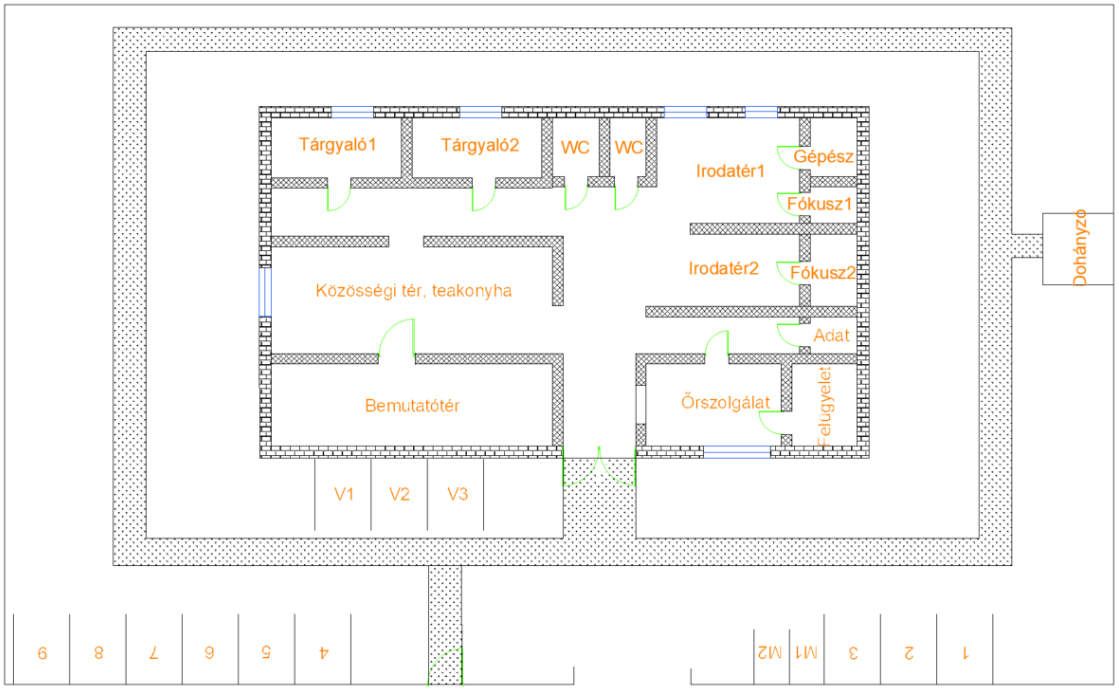
Az objektumvédelem kialakításával érintett fiktív épület tulajdonosa a FutureAi Kft. (a továbbiakban: Kft.), mely portfóliója szerint biztonságtechnikai- és elektronikai szórakoztató eszközök forgalmazásával, valamint részben különböző szoftverek fejlesztésével foglalkozik. A céget pár éve alapították. A székhelyéül szolgáló létesítmény egy kisváros külső részén található, kivitelezése közel húsz éve valósult meg. A telek,

melyen az épület is található negyvenöt méter hosszúságú és ötven méter szélességű, összesen kettőezer-kétszázötven négyzetméter alapterületű. Sík terepen fekszik és szervízúton megközelíthető, a közvilágításon kívüli egyéb közművek kiépítésre kerültek. Közvetlen környezetében üres, beépítetlen, de értékesíthető telkek találhatóak, illetve tágabb környezetében fás-bokros növényzet a jellemző. A cég jövőbeni terjeszkedési stratégiájában rögzítette előbbi területek megvásárlását, amennyiben tevékenységük pénzügyileg jövedelmező lesz és kedvező profitot érnek el. Tervük szerint új irodaépületeket, raktárakat, zöldfelületi közösségi tereket hoznának létre és azokat egy nagyobb telephellyé olvasztanák össze. Előbbi oknál fogva a meglévő objektumon az optimális védelem kiépítése a cél az ár-érték arányok figyelembevételével, mivel nagyobb telephely kialakulása esetén a korszerűbb biztonságtechnikai eszközökre való frissítés jelentős költséget jelentene. A jelenleg rendelkezésre álló önálló, földszintes kialakítású épület háromszázötven négyzetméter, teherhordó szerkezete hagyományos téglából készült, néhány nyílászáró ablak található a homlokzatain. Egyik oldalról sem határolja egyéb épületszerkezet, körbe sétálható a széles betonozott gyalogos- és zöldsávnak köszönhetően. Funkcióját tekintve irodaépület, melyben a cég jelenleg húsz fő munkavállalót foglalkoztat, ezt a későbbiekben harminc főre szeretnék kibővíteni. A forgalmazott eszközök tárolását és értékesítését jelenleg külső raktár igénybevételével valósítják meg. A telken a cég biztosítani kívánja a parkolást az épület környezetében kialakítva. Elképzelésük szerint a dolgozók 9 db-, a vezetőség 3 db parkolóállást fognak tudni igénybe venni, illetve 2 db motorkerékpár helyezhető biztonságba.

Az épület helyiségeinek kialakítása és elrendezése során fő szempont volt a területek alaprajzi logikai és funkció szerinti elosztása, ezzel megtámogatva a védelem hatékony megszervezését. Ugyanakkor szükséges volt a modern kor szellemének megfelelő, vagyis a munkavállalói hatékonyságot, motivációt elősegítő, ergonomikus munkakörnyezet kialakítása is. Előbbi aspektusokból kifolyólag eltérő funkciójú terek létrehozása valósult meg az irodaépületen belül.

Amin fentebb már említettem az irodaépületet szervízúton közelíthetjük meg és innen is jutunk be a telekhatáron belülre. Az épület egy főbejárattal és egyben belépési-menekülési útvonallal rendelkezik, mely után közvetlenül portaszolgálati pult és

őrszolgálati- részben rendszerfelügyeleti helyiség található. Az irodatérbe és a kisméretű tárgyalókba a portától tovább haladva jutunk el. Ezen helyiségekben történik a konkrét munkavégzés, melyet asztali számítógépeken végeznek a munkavállalók. Kialakításra került az üzleti partnerek és vendégek számára a forgalmazott termékek megtekintésére szolgáló térrész, az ún. showroom (magyarul bemutató tér). Az új ötletek megvitatására és a monitor előtti munkavégzés közben tartandó szünetek eltöltésére a közösségi térben elhelyezett kanapék, továbbá az ételek melegítésére és kávézásra szolgáló teakonyha áll rendelkezésre. A cég tevékenységét tekintve részben szoftverek fejlesztésével is foglalkozik, ezért kritérium volt egy adatszoba kialakítása az elektronikus információk védelme érdekében, mely közvetlen az őrszolgálati helyiség mellett helyezkedik el. Az épületüzemeltetési-, vagyis gépészeti helyiség az épület egyik sarkában került elválasztásra, ahol a belső infrastruktúra, mint például a használati melegvíz, légkezelő és hűtő-fűtő berendezések kezelőszerveit, kijelző egységeit találjuk. Ennek szomszédságában a férfi és női mosdó található. Az objektum jellemzőinek és kialakításának összefoglalását a 2. ábra szemlélteti.



2. ábra: A fiktív objektum sematikus alaprajza [Saját kép]

2.2. Kockázatazonosítás és elemzés

Az objektum bemutatása során részleteztem annak elhelyezkedését, miszerint kisváros külső területén helyezkedik el sík terepen, szervízúton lehetséges megközelíteni, a környezetében üres telkek találhatóak fás-bokros növényzettel és a közvilágítás nincs kiépítve. A következő alfejezetekben azonosítom az épületet és annak tágabb környezetét, érintőlegesen a tűzvédelmi biztonság kérdését, illetve a vagyonbiztonságot befolyásoló kockázatokat és szubjektívan elemzem azok várható bekövetkezésének valószínűségét.

2.2.1. Az épület környezetének elemzése

Az objektum megközelítése során napközben jó látási viszonyok mellett a forgalom akadálymentesen haladhat és rendkívüli esemény bekövetkezésekor (dolgozói rosszullét, tűzeset) a reagáló erők gyors kiérkezése biztosított. A telekhatár mentén a gyalogosok, sportolók, túrázók szemmel jól láthatóak. Éjszakai viszonylatban már megjelennek biztonsági kockázatok, ugyanis kivilágítás hiányában romlanak a látási viszonyok. A közlekedési eszközök és gyalogosok haladását a környezeti hatások (csapadék, jég, sár, lehulló falevelek) tovább ronthatják. [4]

A telekhatár megközelítése és ezáltal az épület megfigyelése, biztonságának elemzése könnyű célpontot jelenthet a támadónak azon oknál fogva is, mivel nem beépített környezetben helyezkedik el az objektum, ezáltal külső térfigyelő kamerák sem állnak rendelkezésre, továbbá nem mérvadó a gépjármű- és gyalogosforgalom sem. A telekhatáron keresztüli illetéktelen bejutás további rizikót (járműlopás, rongálás) jelent, elsősorban a tervezett parkolóban várakozó járművek, másodrészben az épület integritásával (szabotázs, betörés, adatlopás, garázdaság) kapcsolatban. Az érintett település bűnügyi statisztikája az elmúlt években nem mutat nagyszámú és súlyos eseményeket, ezen belül kriminalisztikai jelentések száma elhanyagolható. Kisebb szabálysértésekből minden hónapban bekövetkezik tíz és húsz érték közötti esetszám, azonban a (főleg vagyon ellen elkövetett) bűncselekmények száma és súlya éves szinten is csekély mértékű. A közbiztonság állapota megfelelő, a helyi rendőrkapitányságon megfelelő számú és felkészültségű rendőr teljesít szolgálatot. A békés kisváros jelleget tovább erősíti, hogy a helyi lakosok ismerik egymást és összetartó közösséget alkotnak,

ezáltal ha rendkívüli esemény történik, akkor a rendőrség munkáját a település több pontján elhelyezett térfigyelő kamerákon kívül a helybéliek is, illetve a nemrég alakult polgárőrség is hatékonyan tudja segíteni. [4]

2.2.2. Az épület tűzvédelmi biztonsága

Jelen dolgozatomban - amint azt már a Bevezetésben is említettem – érintőlegesen foglalkozom tűzvédelmi kérdésekkel.

Az életvédelem mindig elsőbbséget élvez a vagyonvédelemmel szemben. Az épület tűzvédelmének és tűzjelző eszközeinek kialakítása, üzemeltetése és karbantartása kritikus jelentőségű és a hatóság által ellenőrzött tevékenység. A jogszabályok be nem tartása közvetlenül veszélyeztetheti az élet- és vagyonvédelmet, továbbá jelentős tűzvédelmi bírságokat vonhat maga után. [4] [7]

Az objektum elhelyezkedése szerint kiesik a település középpontjából, ezáltal a beavatkozó erők (hivatásos- és önkéntes tűzoltóság) reakcióideje arányosan meghosszabbodik a távolság és az esetleges rossz időjárási körülmények, valamint a közúti forgalom leterheltségétől függően.

A természeti katasztrófák kialakulása egyáltalán nem jellemző a térségre. A villámcsapások általi épületkár kialakulásának kockázata is kis mértékű, mivel az épület tágabb környezetében találhatóak magasabb épületek is. Egyedüli külső veszélyforrásként a nyári csapadékmentes időszakban a száraz növényzet meggyulladását lehet számításba venni például egy eldobott égő cigaretta által. Az épületben tilos a dohányzás, csak az erre a célra kijelölt külső dohányzó vehető igénybe.

Pozitívumként értékelendő, hogy az épület falazata hagyományos téglából épült, mely jó tűzállósági értékkel rendelkezik. Az épület méretéből, kialakításából, irodai funkciójából, a benne található helyiségek rendeltetéséből és számából kiindulva tűzvédelmi szempontból a leginkább veszéllyel érintett épületrészegységek az adatszoba és a gépészeti helyiség. A szerverek folyamatos működtetése során azok nagyobb hőterhelésnek lehetnek kitéve, ezáltal egy esetleges rövid zárlat megnövelheti a tűz

kialakulásának kockázatát. Azonban a cég méretét és tevékenységi körét figyelembe véve csak kisebb teljesítményű szerverek, adattároló szekrények telepítése indokolt. [4] [7]

A teakonyhában, tárgyalókban, közösségi térben, irodatérben, bemutató térben a biztonságot veszélyeztető tényező lehetnek emberi mulasztásból fakadóak. Ide értendő az elektronikai eszközök villamos felülvizsgálatának hiánya (például a számítógépek, monitorok kábeleinek sérült védőszigetelése vagy a hálózati elosztóba beletört mobiltöltőfej pinek) miatti tűz vagy rövid zárlat kialakulása. A keletkező tűz gyorsan átterjedhet más helyiségekre vagy akár az egész épületre is. A cég tevékenysége közé tartozik részben a szoftverfejlesztés is, amire néhány munkavállalót foglalkoztatnak. Tevékenységüket nagyobb teljesítményű és ezáltal több energiát fogyasztó asztali számítógépekkel végzik, de nem folyamatos jelleggel, ezáltal az eszközök túlmelegedésének kockázata véleményem szerint alacsony kockázatú. A részletezett tűz keletkezést kiváltó okok előfordulása igen alacsony. [4] [7]

Az objektumban található helyiségek elrendezése és az azokba vásárolt bútorzat mennyisége és minősége okán az előző bekezdésekben részletezett események bekövetkezésének hiányában egyéb tűzzel kapcsolatos kockázat nem azonosítható. Az épület védelmének kialakítása során kellő figyelmet kell fordítani a tűzvédelmi kérdésekre és a jogszabályokban meghatározott követelményeknek minden esetben eleget, de célszerűbb többet is tenni. [7]

2.2.3. Az épület vagyonvédelmi szempontú biztonsága

Ebben a részben a védendő objektumot vagyonvédelmi szempontok alapján elemzem. A Kft. profiljának konzekvenciája, hogy a biztonsági kockázatok a következő tevékenységek köré csoportosulnak: betörés, lopás, szabotázs, anyagi javak megrongálása, adat- és információ eltulajdonítás, ipari kémkedés. A cég székhelye szerinti térségben, illetve magában az országban terrorista jellegű csoportok és általuk elkövetett bűncselekmények (robbantás, személyek túszul ejtése, emberölés) nem jellemzőek, illetve a korábbi évtizedekben sem kerültek rögzítésre. [11]

Korábban már bemutattam az épület környezetének biztonságát és elöljáróban kijelenthető, hogy pozitív korreláció áll fenn. Ez azt jelenti, hogy amennyiben megnő a telekhatáron a fenyegetettség veszélye, az megemeli az épület biztonságának sérülékenységét is. A részben izolált elhelyezkedés, észrevétlen megközelíthetőség és a közvilágítás hiányának okán a támadónak lehetősége és több ideje van az objektum felderítésére. [4]

A bűnügyi statisztikák ugyan kedvezőek a biztonság szempontjából, azonban a cég tevékenységi körét figyelembe véve magas kockázatot jelent az ipari kémkedés. Elsősorban hasonló orientációjú vállalatok, startup cégek (magyarul innovatív, gyors növekedési potenciállal rendelkező vállalkozások) részéről vagy azok által felbérelt támadókon keresztül valószínűsíthető ilyen jellegű incidens elkövetése. Megvalósulhat konkrét betörés által (, ugyanis a földszintes kialakítás és körbejárhatóság megnöveli a választható behatolási pontok számát), de akár inkognítóban az épületbe jutva is. Hasonló kockázat lehet a bemutató térben elhelyezett modern elektronikai eszközök lopási kísérlete. Utóbbi tevékenység alatt nem csak az eszköz fizikai eltulajdonítását érthetjük, hanem a piacon még nem elérhető technikáról vagy technológiáról készített kép- és hanganyagok készítését is. [11]

Fenti cselekmények nem kizárólag külső támadás során valósulhatnak meg. A belső fenyegetettségre való felkészülés szintén sarkalatos pontja a kialakítandó védelemnek. Ezen jellegű kockázat részben a munkavállalókon keresztül, másodrészben az épületben sorozatos jelleggel belépő, de legálisan ott tartózkodó alvállalkozók (üzemeltetési, karbantartási, kivitelezési, őrzési, takarítási) munkavégzése során realizálódhat. A kívülről jövő támadáshoz hasonló események prognosztizálhatóak. Megvalósulhat szándékos, rosszindulatból elkövetett és nem szándékos, vagyis emberi mulasztásból fakadóan is. Jelentős kockázatot jelent az adatlopás- vagy szivárogtatás, ami közvetett (külső merevlemez eladása, kártékony szoftver telepítése) és közvetlen módon (a munkaállomásnál felügyelet nélkül hagyott számítógép, dokumentum), fizikális vagy digitális szabotázs (munkaeszközök és kiállított elektronikai eszközök megsemmisítése vagy szenzibilis információk, szoftverek, szerződések törlése). Előbbiek akár

megvalósulhatnak a bemutató térbe szervezett havi rendszerességű látogatások alkalmával a felügyelet nélkül hagyott vendég által is. [4] [11]

Az objektum védelmében kulcsszerepet tölt be a széleskörű belépési jogosultsággal rendelkező őrzést ellátó személyzet. Feladata az incidensek megelőzése, a negatív következmények minimalizálása, vagyis az ellentevékenység végrehajtása (lopás, betörés megakadályozása, stb.). A szolgálat adás közbeni esetleges mulasztás jelentős anyagi kárt okozhat a Kft.-nek, mint például a felügyeleti kíséret nélkül hagyott alvállalkozó vagy a járőrözési terv be nem tartása. Fontos számításba venni, hogy a pozitív kulcsszerep hamar átfordulhat negatív irányba is. Erre precedenst teremthet, ha a telekhatáron belüli belépési hozzáférést vagy kártyát, kulcsokat, nagy értékű ingóságokat átadja harmadik fél számára. A Kft. megbízható vagyonőri szolgáltatót kíván alkalmazni, de ez nem zárja ki a pozícióból eredő visszaélés lehetőségét. [11]

A biztonsági kockázatok összegzéseként elmondható, hogy a megfelelő közbiztonsággal rendelkező településen elhelyezkedő kisebb alapterületű objektumoknál is számos fenyegetési változót kell számításba venni. A több emeletes és modern épületeknél is hasonló fenyegetettségek állnak fenn, csupán a méretbeli és dolgozói létszámbeli különbségeknél fogva a védelem megtervezése és kiépítése több időt, biztonságtechnikai eszközt és magas szakmai tapasztalatot kíván meg. A támadásoknak többféle célkitűzése lehet: kisebb vagy nagyobb vagyoni kár okozása, haszonszerzés, ipari kémkedéssel versenyhátrányba kényszerítés, üzletmenetfolytonosságban való zavar keltés. Ahogyan már a korábbi fejezetben is említettem, az őrzés folyamatos ellentevékenység, mely akár évekig is eltarthat negatív esemény bekövetkezésének hiányában. Incidens bármikor kialakulhat, ezért az objektum felügyelete alatt a figyelemnek nem szabad lankadnia, folyamatos készültségi állapotban tartása fontos követelmény. Az előzőekben említett tudatos vagy emberi mulasztásból eredő támadásokra fel lehet előzetesen készülni és ezáltal hatékony, de arányos védelmet és intézkedési folyamatot kialakítani. Ehhez azonban szükségünk van a védendő objektum biztonsági szempontú elemzésére, ami alapot ad a kockázatértékelés elkészítéshez. [4] [33]

2.3. Az objektum kockázatértékelése

Az előző fejezetben elvégeztem a kockázatazonosítást és elemzést, melynek során az objektum jellemzőit figyelembe véve kitértem a lehetséges negatív eseményekre, azok hatásaira és valószínűségére. Az incidensek jellege, intenzitása és a cégre gyakorolt hatása sok tényezőtől függ és szignifikánsan eltérhetnek egymástól. Az értékelés elvégzéséhez a kvalitatív módszert alkalmazom, ehhez azonban először meg kell határozni néhány szempontot. [34] [35]

2.3.1. A kockázati mátrix

Fontos deklarálni, hogy a mátrix az objektum jelenleg ismert kockázatait veszi figyelembe. A környezetében és magában az épületben, vagy az abban végzett tevékenységben bekövetkezett jelentősebb változás esetén célszerű lehet frissebb, aktualizált kockázatértékelést készíteni. A módszer első lépéseként a korábban részletezett kockázatelemzés alapján kategorizálom a fenyegetéseket. Értékelem az esemény bekövetkezésének gyakoriságát, azaz valószínűségét (jelölése: V), majd annak hatását, vagyis az okozott kár mértéket (jelölése: H). Ezek súlyozott pontozását egytől ötig terjedő skálán rögzítem (nagyon alacsony-alacsony-közepes-magas-kritikus). A két szempont szorzatából kapott összeg egytől huszonötig tartó tartományban adja meg a kockázati súlyosságot (jelölése: K, az egyenlet szerint K = V x H). A minősítés értelmezését követően konkrét védelmi javaslatok kell kidolgozni. [32] [34]

Az elemzésemet alapul véve az objektumot veszélyeztető eseményeket hat fő csoportban összegzem:

1. Természeti-, és környezeti tényezők (vihar, száraz növényzet miatt tűz kialakulása, gyújtogatás).
2. Műszaki meghibásodások, üzemzavarok (rövidzárlat, csőtörés, tűzeset, áramkimaradás).
3. Humán jellegű tényezők (nyitva hagyott ajtó, zárolatlan számítógép, jelszavak továbbadása).
4. Szervezeti tényezők (kontrollálatlan beléptetés, hanyag kulcskezelés, gondatlanság, adatszivárogtatás).

5. Külső támadások (betörés, gépjármű- vagy eszközlopás, ipari kémkedés, bemutató tér eszközeinek rongálása, szabotázs).
6. Belső támadások (rongálás, adatlopás, szabotázs).

A kategorizálás után mindegyik ponthoz a valószínűség és hatás értékszámát is hozzá kell rendelni. Az elemzésemből kiindulva a kategóriák első felében négy, tizenkettő-tizenkettő, míg a második felében tizenkettő, húsz és huszonöt kockázati értékszámokat kaptam.

A táblázati adatok kockázati mátrix létrehozásával vizuálisan jobban szemléltethetőek. A különböző kockázati szintek jelölésére általában zöld-citromsárga-narancssárga-piros-bordó színkombinációkat szokás használni, illetve professzionálisabb kinézet elérésére hőtérkép is alkalmazható. A 3. ábrán az egyszerűsített kvalitatív módszerrel megalkotott mátrix látható a kockázatelemzés végeredményeként. [32] [34]

Kockázati kategória	V	H	K
1. Természeti- és környezeti tényezők	2	2	4
2. Műszaki meghibásodások, üzemzavarok	3	4	12
3. Humán jellegű tényezők	3	4	12
4. Szervezeti tényezők	3	4	12
5. Külső támadások	4	5	20
6. Belső támadások	3	5	15

1-5	6-10	11-15	16-20	20-25
Nagyon alacsony	Alacsony	Közepes	Magas	Kritikus

3. ábra: A kockázati mátrix [Saját szerkesztés]

2.3.2. A kockázati mátrix elemzése

A kockázatértékelési folyamat a mátrix értelmezésével zárul le és egyben előkészíti a kockázatkezelést. A táblázat és a mátrix rávilágít arra, hogy az azonosított kockázatok súlyosságai eltérőek és különféle módokon befolyásolhatják a Kft. működését. [32] [34]

Kritikus kockázati kategória szerint a legnagyobb előfordulási eséllyel és okozott kárral az információ- és adatlopás, ipari kémkedés érintett. Eme kettő támadás kritikus jelentőséggel bír nemcsak az üzletmenet folytonosságának integritására, de a céget

reputációs veszteség is érheti. A cég közvetlen és közvetett közelében nincs hasonló tevékenységi körrel foglalkozó egyéb vállalat, azonban a piaci verseny okán az adatlopás kritikus tényező, ami ellen a Kft.-nek létszükséglete a védekezés.

Magas kockázati kategóriába a betörés, rongálás, szabotázs akciók kerültek, habár a térség bűnügyi statisztikái nem indokolják ezt. Azok a tények, hogy a védendő objektum részben elszigetelt területen helyezkedik el, földszintes kialakítású és a megközelítési útvonal nem rendelkezik közvilágítás kiépítettséggel sem térfigyelő kamerarendszerrel, tovább erősítik a fenyegetettséget. A külső támadót nehezebb detektálni. A kockázati besorolás igazolja, hogy belsős ember is elkövetheti a rongálást, szabotázst. A munkavállaló a napi tevékenysége során kellő helyismereti tapasztalatot gyűjthet, a kollégák és azok napi rutinjának feltérképezésével könnyen végrehajthatja azt. Bekövetkezési valószínűségük alacsony, az okozott hatás magas. [4]

Közepes kategóriába tartoznak a műszaki meghibásodások, üzemzavarok, emberi mulasztásból származó kockázatok és a szervezeti eredetű tényezők. Valószínűségük alapján ritkán és közepes gyakorisággal is előfordulhatnak, azonban kellő figyelemmel, felügyelettel, karbantartással vagy a dolgozóknak előírt és kötelezően elvégzendő munkavédelmi, tűzvédelmi, biztonsági és érzékenyítési tanfolyamok által viszonylag könnyen kezelhetővé válnak. Megvalósulások esetén az okozott kár magas lehet. [35]

Alacsony kockázati értékkel az időjárás okozta károk, az objektum környezetében esetlegesen keletkező tüzek bírnak. Előfordulások szerint ritkán vagy soha nem fognak veszélyt jelenteni, de minimális kockázattal így is számolni szükséges. Megfelelő karbantartói felkészültséggel, intézkedési láncolatok létrehozásával az esetleges károk is nagymértékben minimalizálhatóak.

A fejezetben a védendő objektum bemutatásával azonosítottam, részleteztem és szubjektíven megítéltem a kockázatok előfordulási valószínűségét és hatását. Bemutattam a kockázati mátrixot és elemeztem a kapott értékeket. A következő pont a kockázatkezelés, melyben biztonságtechnikai eszközöket javaslok. A biztonság alapú elemzést tekintve jelen, de logikailag és tartalmilag a következő fejezethez tartozik.

3. FIZIKAI VÉDELMI RENDSZEREK TERVEZÉSE ÉS INTEGRÁCIÓJA TECHNIKAI ESZKÖZÖKKEL

A kockázatazonosítást és elemzést követően ebben a fejezetben a kockázatkezelést mutatom be. A folyamat célja, hogy az elvégzett vizsgálatok során kapott kockázati eredmények alapján a védelmi eszközöket és intézkedéseket meghatározzuk. Komplex vagyonvédelmi rendszer tervezéséhez átfogó szakmai gondolkodásmód és kellő tapasztalat szükséges, továbbá a korábban említett szakterületek bevonása is elengedhetetlen. Ahogyan azt már az első fejezetemben részleteztem, az objektumvédelem három darab részegységből épül fel. Ezek közül jelen fejezetben kizárólag a mechanikai védelemmel, elektronikai jelzőrendszerrel, illetve védelmi zónarendszer koncepciójával foglalkozom. A hat darab kockázati kategóriához arányos védelmi megoldásokat javaslok, de a kapcsolódó szabványokat, ajánlásokat és jogszabályokat nem részletezem. A rendszer komplexitásának harmadik pillérét adó élőerős őrzést, annak lényegét, működését, kialakítását a negyedik fejezetben taglalom. [32] [37] [38]

3.1. A kockázatkezelés és a védelmi zónarendszer

A kockázatazonosítás kimutatta, hogy a Kft. esetében széles spektrumon elterülő kockázati eseményekre kell felkészülni a kockázatkezelés során meghatározandó védelemnél. A biztonságtechnikai eszközök célja, hogy támadás vagy fenyegetés esetén, ha a visszatartó- vagy elrettentő erő nem bizonyult elégségesnek, akkor a megelőzésben, a támadó detektálásában és feltartásában hatékonyan működjenek közre. A kockázatelemzés során meghatározott kategóriák segítségével pontosan meg lehet határozni az optimális védelem kialakításához szükséges eszközöket és intézkedéseket. Minél nagyobb a kockázat és annak bekövetkezési valószínűsége, annál átgondoltabb védekezést kell felépíteni, ami nem minden esetben egyenesen arányos a költségek és intézkedések növekedésével. [32] [34] [38]

A kockázatkezelés során javasolt védelem hatékonysága nem permanens, mivel a kockázatok folyamatosan változhatnak (profil váltás, környezet változása, új támadási

technikák), ezért időszakonkénti felülvizsgálatra szorul. Azonban néhány fontos tervezési intézkedéssel alapvető, hosszabb távon is jól működő védelmi rendszert hozhatunk létre, mint például a védelmi zónák strukturális elvének felhasználása és gyakorlatba történő átültetése, kialakítása. Az objektumban való zónarendszer létrehozásával a meghatározott kockázati szinteknek megfelelő ellentevékenységek sorozata szabályozható le. [8]

A védelmi zónák létrehozása jelentős szerepet játszanak a komplex fizikai védelem kialakításában. Céljuk, hogy az objektum részeit képező egységeket az előre meghatározott biztonsági szintbe soroljuk be. Az adott részegység, helyiség zónájának meghatározása a személyi belépési jogosultság, a védendő érték, adat és a kockázati szint figyelembevételével valósul meg. A zónaszint számoknak nincs alsó vagy felső számbeli korlátozása, azonban dolgozatomban nulladiktól a harmadik szintig különböztetem meg, vagyis a legkisebb kockázattal érintettől a kritikus fenyegetettségig. A biztonsági modell alkalmazásával gyűrűs- vagy másnéven mélységi védelmet alakíthatunk ki, tehát a külső alacsony szintű zónától a támadónak fokozatosan nehezebb dolga lesz átjutni a következő, magasabb szintű és összetettebb védelmeken. [37] [38] [8]

3.1.1. Természeti-, és környezeti tényezők

Az objektum környezeti adottságai, vagyis a részben izolált elhelyezkedés, megközelítés, beépítetlen környező telkek, illetve a természeti eredetű kockázatok alacsony valószínűséggel fordulhatnak elő. A növényzet szikra általi belobbanásával keletkezű tüzek, villámcsapások, extrém mennyiségű csapadék lehullása következtében kialakuló villámárvíz, szélvihar jelenthet fenyegetettséget elsősorban az épület integritására, majd az abban tartózkodók épségére.

Mechanikai védelem szempontjából hatékony védelem alakítható ki a telekhatár lehatárolását szolgáló kerítéssel. A típusát tekintve javasolt a szilárd, pontheggesztett kivitel és a leküzdést nehezítő sűrű rácsozás. Az épületen kívüli térrészek és a környező területek növényzetének kaszálása, villámhárító rendszer kiépítése, csapadékvíz-elvezető árkok és víznyelők hordalékmentesítése és karbantartása, jó minőségű zárt szerkezetű nyílászáró alkalmazása és a tetőszerkezet időszakos állapotellenőrzése jelentősen csökkenti az esetleges károk hatását. [7]

Elektronikai védelem aspektusából a meteorológiai jelzőrendszer (csapadék, hőmérséklet, szél,) preventív értékkel bír, segítségével a megelőző és beavatkozó intézkedések ideje jelentősen lecsökkenhet. A természeti és környezeti eredetű eseményekre kerítés által nyújtott biztonságot tovább fokozza az épület sarokpontjaira applikálandó, egymásra rálátó CCTV kamerarendszer egységei, illetve analitikai funkció esetén a nem szokványos mozgások detektálásával a terület folyamatos monitorozása valósul meg, A közvilágítás hiányából fakadóan a kerítésrendszert érdemes mozgásérzékelők és LED lámpák kombinációjával megtámogatni. [7] [34]

Zóna besorolás szerint nulladik szint az irányadó. Ezen kategória nem igényel túlzott, sokrétegű védelmi ellentevékenységet, mivel az objektumon kívülről számítunk incidensre, illetve a korábban felsorolt eszközökkel és intézkedésekkel a kockázatok megelőző jelleggel kezelhetőek. Utóbbiak viszont az elsődleges védelmi vonal elengedhetetlen részét képezik. A telekhatáron és az épület közötti terület egyes szintű besorolással érintett. Belépési jogosultság szempontjából általános védelmi zóna, vagyis a kerítésen belépési pontként kártyaolvasóval szerelt belépőkaput vagy biztonsági ajtót és automata, esetleg rendszámfelismerő kamerával kiegészített sorompót kell kialakítani. Utóbbi esetében ún. sorompószakállal való kiegészítés is javasolt, ezáltal a sorompókar alatti réseken való bejutás kivédhető. A telephelyen az éjszakai munkavégzés hiányában erősen indokolt az objektum határainak lezárására, mégpedig a gépjárműforgalmat megakadályozó tolókapu applikálásával. A tervezett eszközök használatával hozzáférési jogosultság alapján szabályozott az objektumba történő be- és kilépés. Javasolt a modern, vezetéknélküli rádiófrekvenciás azonosítási (angolul Radio Frequency Identification, röviden RFID) technológiát használó kártyaolvasókat telepíteni és belépő kártyákat alkalmazni. A hozzáféréssel nem rendelkező vendégek részére kaputelefon létesítése javasolt, mely az őrszolgálathoz rendelkezik közvetlen bekötéssel. [7] [34]

3.1.2. Műszaki meghibásodások, üzemzavarok

Műszaki jellegű kockázatként a rövidzárlat, rövidebb vagy hosszabb távú áramkimaradások, tűzesetek, épületgépészeti meghibásodások kerültek azonosításra, melyek elsősorban, de nem kizárólag az adatszobára és a gépészeti helyiségre jelenthetnek veszélyt. Ezen épületrészek folyamatos működéssel érintettek,

következésképpen folyamatos áramellátásre, hűtésre, szellőztetésre és zavartalan üzemre van szükségük. Bekövetkezési valószínűség nem magas, de az okozott hatás kritikus lehet a cég üzletmenetfolytonosságában, adatbiztonságában. [7] [34]

Műszaki védelmet tekintve alapvető a berendezések megfelelő karbantartottsága, sértetlen burkolatok és védőszigetelések állapota, stabil rögzítése. A fizikai biztonság kialakítására és megőrzésére a helyiségeket elkülönítetten, zárva, kívülről gombos és belülről kilincses megoldással szerelt biztonsági ajtóval, beléptető kártyaolvasóval esetleg mechanikai kulcsos zárszerkezettel felszerelve kell létrehozni. Mindkettő helyiségben a megfelelő hőmérsékletről, szellőztetésről (esetleg páratartalomról) gondoskodni kell. A gépészeti helyiség esetén mechanikus szellőztetés, vagyis gépészeti elszívás és frisslevegő utánpótlás elégséges, az adatszobára szabványi követelmények vonatkoznak. A védendő szerverhelyiség kisebb méretű, ezért redundáns hűtő-fűtő inverteres split klíma telepítése elegendő. [7] [34]

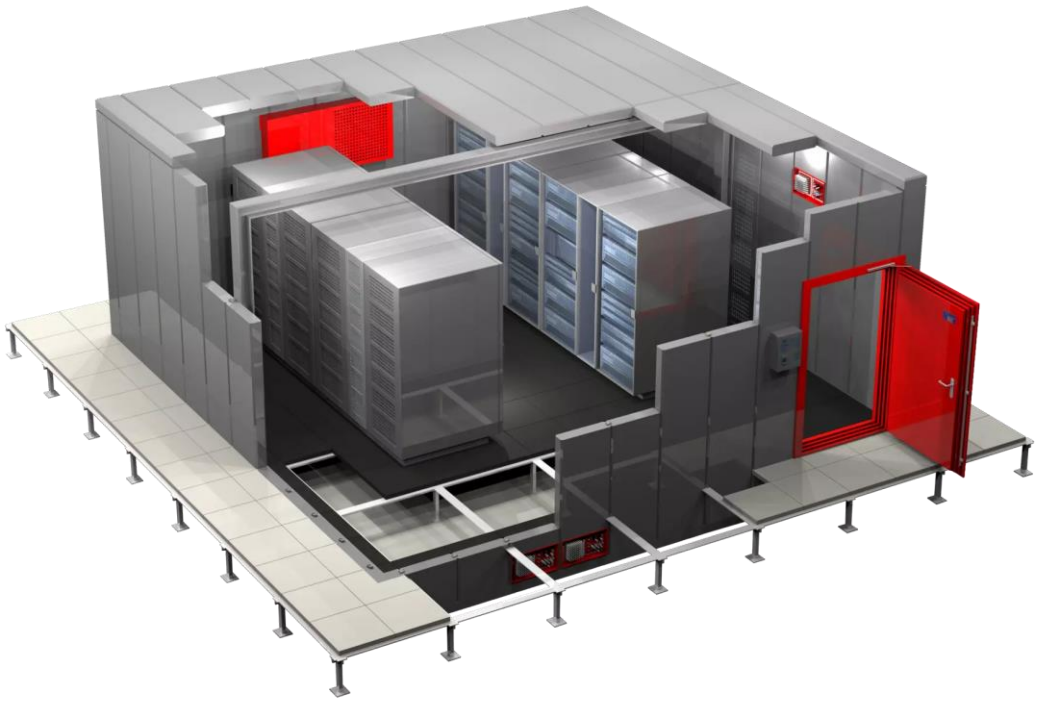
Az elektronikai rendszereket tekintve fontos a két helyiség monitorozása hőmérséklet, klíma szempontjából a berendezések túlmelegedésének elkerülése érdekében. Ezen megfigyelő rendszerek gyorsabb reagálást tesznek lehetővé és egyben a szoftveres naplózás általi statisztika felállítását támogatják, ugyanakkor költségesebbek és meghibásodás esetén közvetve súlyos károkat okozhatnak. Megfelelő szervezeti intézkedésekkel például őrjáratok és fizikai naplók rendszeresítésével kombinálhatóak vagy kiválthatóak. Az áramkimaradások okozta esetleges szerverleállások vagy gépészeti hibák elkerülésére kellő teljesítménnyel rendelkező szünetmentes tápegység (Uninterruptible Power Supply, röviden UPS) alkalmazásával mérsékelhetjük a kockázatot. [7] [34]

Tűzvédelmi szempontból csak érintőlegesen foglalkozom az objektummal. Az alábbi kockázatkezelési javaslatok a további kockázati kategóriákkal is összefüggésben állnak, mivel a tűz elleni védekezés során az egész épületet és annak környezetét is szükséges vizsgálni. A vonatkozó jogszabály, vagyis „*az Országos Tűzvédelmi Szabályzatról”* szóló 54/2014. (XII.5.) BM rendelet mellékletei, illetve a Tűzvédelmi Műszaki Irányelvek alapján az épület kockázati besorolása, a passzív tűzvédelme, a szükséges tűzvédelmi

berendezései pontosan meghatározhatóak. Ezek szerint a védendő objektum NAK (nagyon alacsony kockázati osztály) besorolásba tartozik. A meghatározást a következő jellemzők biztosítják: földszintes kialakítás, hagyományos tégla falszerkezet, háromszázötven négyzetméter alapterület, iroda funkció, alacsony a helyiség négyzetméter aránya, kisebb méretű és alacsonyabb terheltségű adatszoba és gépészeti helyiség, nincs tűzveszélyes tevékenység és túlzott éghető bútor használat, húsz és harminc fő között változhat az egyszerre az épületben tartózkodók és önállóan menekülni képesek létszáma, a helyiségek elhelyezkedése alapján a menekülés szabad térre egyszerű és gyorsan végrehajtható és éjszakai munkavégzés nem történik. [7] [18] [34]

Ellenben fenti felsorolás alapján a menekülési útvonalat vészvilágítással és irányfényekkel kell jelölni, áramkimaradás esetén a beépített akkumulátor biztosítja az áramforrást. Az épület elhagyása az őrszolgálat, illetve a porta felé történik a beléptető kapu kiegészítéseként telepített pánikzár funkcióval ellátott lengőkapun keresztül, mely anyagmozgatás során is használható. A belső beléptető rendszerre a vésznyitás funkciójaként vészkikapcsoló gomb applikálása is szükséges, melynek aktiválása során például a forgóvillák karleesés üzemmódba váltanak át és szabad átjárást biztosítanak. A külső szabad térbe való jutás az épület biztonsági, duplaszárnyú, szintén pánikzárral szerelt ajtaja után valósul meg. [7] [18] [34]

Érdemes a Kft. vezetésének megfontolni, hogy az adatszoba és a gépészeti helyiség biztonságát növelve megfelelő tűzállósági értékkel rendelkező tűzgátló ajtót, tűzálló falazatot és kézi jelzésadót telepítenek. Ebben az esetben a tűzjelző központ az őrszolgálati helyiségben létesülne és hang- és fényjelző eszköz is kötelezően kivitelezendő a tűz keletkezésének jelzésére, illetve hasonlóan beépített akkumulátor szükséges. A tűzjelző rendszer kiépítése habár nem kötelező az objektum paraméterei, funkciója, stb. alapján, de jelentősen növeli biztonságot. Ennek hiányában a tűz jelzésére a munkavédelmi oktatásában kötelező rögzíteni a dolgozók által észlelt esemény információjának továbbadására használandó figyelemfelhívó test- és hangjelzéseket. A 4. ábra az elkülönített és megfelelő védelemmel kialakított adatszobát szemlélteti. [7] [18] [34]



4. ábra: Adatszoba biztonsága [39]

Nincsen szükség automatikus oltórendszerre sem, az épületben esetlegesen keletkező tüzek oltására elegendő kettő darab hat kilogrammos ABC típusú porral oltó készülék. Elhelyezésük jól látható és hozzáférhető hely szerint a teakonyhában és az őrszolgálatnál javasolt. Az adatszoba bejáratánál célszerű önálló öt kilogrammos szén-dioxiddal oltó készülék elhelyezése az esetleges elektromos tüzek megfékezésére. [7] [18] [34]

Zónabesorolás szerint az adatszoba és a gépészeti helyiség a legmagasabb harmadik szintű. A korábban felsoroltak alapján a műszaki meghibásodások és tüzek keletkezésének alacsony a valószínűsége, de jelentős és hosszantartó károkat, életveszélyt is okozhatnak. Ezen épületegységekbe a belépés kizárólag a szükséges magas szintű jogosultsággal rendelkező személyek részére hozzáférhető. A beléptető kártyarendszer és olvasók segítségével a jelenlétek naplózhatok. Az objektum védelmi integritásáért is felelős rendszerfelügyeleti helyiség szintén harmadik biztonsági szintbe sorolandó, hiszen innen könnyedén diszfunkció okozható a további rendszerekben. [34] [8]

3.1.3. Humán jellegű tényezők

Az emberi tényező mindig meghatározó és gyakoribb kockázatokat jelent. Az azonosítás során a zárolatlan számítógép, jelszó vagy belépő kártya továbbadását, hanyagságból őrizetlenül hagyott dokumentumokat, nyitva felejtett ajtókat emeltem ki biztonsági fenyegetettségként, ezek jelentős kárral terhelhetik a céget.

Mechanikai nézőpontból csökkenthetik a veszélyt az automatikával szerelt önzáródó ajtók, kulcstároló széfek által küldött figyelmeztető jelzések a hiányzó kulcsokról. [7]

Elektronikai megoldások terén a védelmet hatékonyan elősegítik a belépések naplózása és azok kamerarendszerrel való megtámogatása. Fontos megjegyezni, hogy csak a belépési pontok és nem munkavégzésre használt objektumon belüli területek megfigyelése engedélyezett. A munkaterületet és a kerítésen kívüli köz- vagy magánterületet a kamerarendszer által rögzített videóanyagból kitakarással kell eltávolítani. [7] [34]

Vagyon- és munkavédelmi szempontból is kiemelt szempont, hogy a munkavállalók folyamatos oktatásokon, tréningeken vegyenek részt. Ezáltal tisztázható az alapvető felelősség vállalása munkájuk és munkáltatójuk irányába, illetve érzékenyítésük a különböző biztonsági események által okozott károk bemutatásával és annak terhelő jogi vonzatával.

A védelmi zóna besorolás ebben az esetben kettes szintű és az őrszolgálatnál elhelyezett beléptetű kapu utáni épület nagyobb részét érinti. Az emberi tényező sosem zárható ki teljes mértékben, de cég általi hatékony kommunikációval, oktatásokkal, prevenciós intézkedésekkel kezelhetővé tehető.

3.1.4. Szervezeti tényezők

Az előző alfejezetben taglaltakkal részben korrelációt mutatnak a szervezeti kockázati faktorok komponensei. Azonban nem kizárólag konkrét személyhez köthető hiányosságokról van szó, hanem rendszerszintű működés okozhat diszfunkciót a cég életében. Az azonosított biztonsági események a beléptetés ellenőrzésével, kulcs- vagy

adatkezeléssel és tárolással, valamint a vendégek és alvállalkozók objektumon belüli kontrollálatlan tevékenységével hozzhatóak összefüggésbe, ezáltal védelmi rések keletkezhetnek. Megfelelő intézkedésekkel a közepes előfordulási tényező és a magas értékű okozott kár csökkenthető.

Mechanikai védelmet kell létesíteni minden fizikai hozzáférési ponton, ahol a jogosultság kérdésköre felmerülhet. Jelentősen redukálható a rizikófaktor kulcskezelő széfek, zárható irattárolók, belépő kapuk létesítésével. Munkatapasztalatom során a kulcskezelés és az alvállalkozók felügyeletének kérdése számos alkalommal kerül megoldandó napirendi pontra. Megoldási javaslat lehet a megfelelő, de nem túlzott mennyiségű épületkulcs, a helyiségek rendeltetésének megfelelő csoportkulcs biztosítása, melyek kártyajogosultság alapján vehetők fel, ezáltal azok mozgása is naplózásra kerül. [7] [34]

Elektronikai jelzőrendszerekkel telepítésének kérdésköre kardinális azon oknál fogva, hogy ezáltal a két védelmi mechanizmus interakciója támogatja egymást. A térfigyelő kamerákkal a be- és kilépési pillanatok visszakereshetőek és egyfajta biztonságérzetet is generál az objektumban tartózkodóknál. A munka felvétele és leadása szintén naplózott formában történik ezek által. [34]

A védelmi zónabesorolás több szintet is érint. Az épületen belüli irodatér, teakonyha, tárgyalók és a bemutató tér második kategóriába esik, mivel általánosabb hozzáféréssel érintett helyiségek. A showroom esete kivételt képez, mivel ide csak az ügyfelekkel való kapcsolattartásért felelős dolgozók rendelkeznek belépéssel, melynek feltételeként külön oktatás elvégzése és a felelősségi körök tisztázása, rögzítése kötelező. Az adatszoba, gépészeti tér és rendszerfelügyeleti helyiség harmadik szintjét igazolja az infrastruktúra szempontjából kritikus jelentőség, a belépés szigorú kontroll alatt tartása elengedhetetlen. A humán tényezőkkel azonosan oktatással, a cég határozott álláspontjával és megfelelő intézkedések, protokollok kialakításával kezelhető és megelőzhető kockázatot kapunk. [38]

3.1.5. Külső támadások

Az objektumon kívülről érkező támadások jelentik a legmagasabb kockázati kategóriát. Az objektum adottságait, a bűnügyi statisztikákat és a cég profilját együttesen megvizsgálva a támadások prognosztizálhatósága a közepesnél magasabb valószínűségi előfordulást és beláthatatlan anyagi károkozást vetít előre. A betörés, gépjármű- vagy eszközlopás, ipari kémkedés, szabotázs és a bemutató térben elhelyezett nagyobb értékű eszközök védelmének kezelése komplex tervezést igényel, aminek alapját az incidens megelőzésére, gyors detektálására és késleltetésére fókuszáló védelmi intézkedések összesége adja. [34] [38]

Mechanikai és az azt megtámogató elektronikai szempontból a korábban is említett eszközök alkalmazása javasolt. A telekhatár menti külső behatolási pontok ellen masszív, közepesen magas kerítés építése, gépjárművel történő behajtás szakállas sorompóval, kártyaolvasóval és tolókapuval való leszabályozása, belépő kapu és annak használata kártyajogosultság alapján, vendégek részére kaputelefon létesítése, munkaidő után aktiválandó mozgásérzékelők vagy kültéri infravonalas mozgásérzékelők LED lámpa kiegészítésével javasolt. A védelem szintjét tovább fokozza a CCTV kamerarendszer által körkörösen védett objektum, különösen ha infravörös képalkotással rendelkezik, így sötétben is hatékonyan alkalmazható. Mesterséges intelligenciával rendelkező típusai képelemző funkcióval is ellátottak, azonban ez magasabb bekerülési költséget is jelent. Alkalmazható az 5. ábrán látható Dome típusú széleslátószögű és nagy felbontású kültéri kamera. A nyílászárók megerősített szerkezete, esetleg töréskésleltetése vagy biztonsági ütésálló fóliázása javasolt. [7] [34]

5. ábra: Dome típusú kamera [40]

A védett adatok és információk következtében a cégnek elemi érdekében áll azok hatékony megóvása. Napjainkban már számtalan hardveres és szoftveres megoldással szolgál a piac, ha adatainkat biztonságban akarjuk tudni. A koronavírus okozta pandémia következtében jelentős mértékben megnőtt az otthonról dolgozók száma, ami a felhőalapú tárhelyek aranykorát hozta magával. Ez azonban számos kiberbiztonsági kockázat megjelenésével is együtt járt. Mind az irodából, mind a távolról történő munkavégzés során elengedhetetlen az adatok védelme érdekében azok felhasználását, továbbítását, kezelését megfelelően leszabályozni, letöltés és továbbítását korlátozni vagy letiltani. Célszerű az irodai számítógépek külső merevlemezhez való csatlakozását külön jogosultsághoz kötni vagy megtiltani és az ilyen tevékenységeket minden esetben naplózni. A tűzfalak, vírusírtók, kémprogram kereső szoftverek használata magától értetődő a céges kultúrában, de sok esetben nem a cég méretéhez igazított minőségi alkalmazások kerülnek megvásárlásra. A szükségtelenné vált bizalmas adatokat tároló merevlemezeket megfelelően, vissza nem állítható roncsolásos adatmegsemmisítés útján javasolt kezelni.

A külső támadások az összes védelmi zónát érinthetik, de a harmadik szintűbe való eljutás a többrétegű védelemnek köszönhetően minden zónát követően nagyobb kockázattal, időveszteséggel és detektálási valószínűséggel jár. Az élőerős őrzés alkalmazása, a belső szabályzók, valamint az incidenskezelő protokollok kiemelt szerepet kapnak a kívülről jövő támadások elhárításában. Az alkalmazandó védelmi eszközök összefogására,

kontrolljára és monitorozására az őrszolgálatnál rendszerfelügyeleti helyiség kialakítása szükséges. [38] [8]

3.1.6. Belső támadások

A külső támadásokhoz hasonló kockázati eseményekre lehet és kell készülni a cég saját alkalmazottai, az alvállalkozók vagy vendégek tekintetében is. Ezen személyek állandó vagy ideiglenes belépési jogosultsággal is rendelkezhetnek és részlegesen vagy teljes mértékben ismerhetik az objektumot, annak gyenge pontjait, a cég és a dolgozók napi rutinját. Ezek következtében könnyűszerrel végrehajtható a fizikai eszköz- vagy elektronikus adatlopás, rongálás, információsziváro gtatás, szabotázs. Valószínűségét tekintve közepes-, míg hatását magas kockázati szintbe soroljuk. [38]

A korábbi kockázati pontoknál felsorolt eszközök, intézkedések jelen alfejezetben is érvényt szereznek alkalmazásukra a hatékonyságuk okán. A műszaki meghibásodások, üzemzavarok kockázati kategóriában tárgyalt biztonsági ajtók, normál vagy fordított működésű zárak, kártyaolvasók és kamerarendszerek jelentik a védelem gerincét. Ezen típusokból is kiemelt fontosságú a minőségi eszközök kiválasztása, ilyen lehet a 6. ábrán látható ajtóbehúzó mechanikával és kulcsos zárszerkezettel ellátott, acélból készült ajtó. Fontos leszögezni, hogy a munkaterületet, egyéb belső térrészeket képrögzítő eszközzel megfigyelni jogszabályi előírások alapján nem lehet. A biztonság azonban tovább növelhető jelenlétérzékelőkkel, nyitásjelzőkkel vagy egyéb riasztó berendezésekkel, illetve a kártyaolvasók esetleges PIN kóddal vagy modernebb biometrikus érzékelővel szerelt változataival. Utóbbi esetben azonban a személyi adatok tárolására és kezelésére vonatkozóan szigorú kritériumoknak kellene megfelelni, ami a Kft. méretéből adódóan jelentős terhet róna, ezért alkalmazása nem indokolt. [7] [34]

6. ábra: Biztonsági ajtó [41]

Minden zónaszintig érheti belső támadás a céget, azonban a legjelentősebb kárral továbbra is az adatszoba és a gépészeti helyiség érintett. A belső támadások megelőzésére a munkavállalók felé történő megfelelő kommunikáció, továbbképzések, a felelősségük tudatosítása és szinten tartatása, a tisztázott belépési jogosultságok alkalmazása a védelmi eszközök integrálásával jelentős védelmi potenciált mutat fel.

A kockázati kategóriákat elemezve mechanikai, elektronikai és szervezet szervezési megoldásokat javasoltam. Ahogy a dolgozatom korábbi részeiben is megfogalmaztam a teljes mértékű, minden eshetőségre felkészített védelem nem létezik, de a biztonság állapotának elérését hatékony tervezéssel és szervezéssel meg lehet közelíteni. A következő fejezetben az élőerős őrzés működését, feladatait, szervezését vizsgálom meg a vagyonvédelmi rendszer elemeként, majd a komplex rendszerben való nélkülözhetetlen jelenlétét és összehangolását dolgozatom utolsó részében mutatom be.

4. ÉLŐERŐS ŐRZÉS SZEREPE ÉS OPERATÍV MŰKÖDTETÉSE AZ OBJEKTUMVÉDELEMBEN

Az eddigi fejezetekben bemutatott kockázatok és kezelésükre javasolt védelmi mechanizmusok rávilágítanak azon tényre, hogy kizárólag a mechanikai és elektronikai jelzőrendszerek önmagukban csak visszatartó erővel bírnak. Késleltetni és jelezni képesek a támadási szándékot, de a tevőlegesen beavatkozás továbbra is emberi jelenlétet igényel, mivel az adott szituációban keletkező anomáliákat még a fejlett mesterséges intelligencia sem tudja minden esetben értelmezni. A következő részben feladataikat, működésüket mutatom be, melyek a dolgozatom témájának választott fiktív épület védelmének meghatározó elemeit adják.

4.1. A vagyonőrzési szolgálat

A helyzetfelismerés és értékelés, a támadóval és a különböző támadási módszerekkel szembeni arányos intézkedések foganatosítása, a vállalatok és cégek érdekeit szem előtt tartó döntések átgondolt, hatáskörrel összeegyeztethető végrehajtása a helyszínen tartózkodó vagyonőrök felelőssége és feladata. Tevékenységüket „*a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól”* szóló 2005. évi CXXXIII. törvény szabta kereteknek, felelősségi köröknek és jogosultságoknak megfelelően kell végezniük. A törvény értelmében csak olyan személy alkalmazható az őrzésvédelem során, aki rendelkezik megfelelő képesítéssel. Ennek megszerzése általában a vagyonőri, testőri képzés elvégzésével valósul meg. A jogszabályban ugyan szerepel a biztonsági őr képzési forma, ez azonban a régebbi rendszerből történeti okok és a hétköznapi köznyelvben használt egyszerűsítés miatt maradt fenn, de jogilag nem értelmezhető. [12]

Fontos megemlíteni, hogy nem csak civil vagyonőrök láthatnak el vagyonbiztonsági, őrző-védő feladatokat. Külön jogszabályok alapján, vagyis *„a fegyveres biztonsági őrségről, természetvédelmi és a mezei őrszolgálatról”* szóló 1997. évi CLIX. törvény, valamint egyéb rendeletek és utasítások alapján a fegyveres biztonsági őr (röviden FBŐ) külön kategóriát képez. Szolgálati helye szerint kiemelt vagy különösen veszélyeztetett

objektumokkal kapcsolatosan lát el őrző-védő tevékenységet. Ilyenek lehetnek például államigazgatási-, honvédségi-, rendőrségi épületek, katonai radar-, kommunikációs- vagy vezetési pontok, repülőterek, diplomáciai kíséretek védelme, kritikus infrastruktúra létesítményei. A vagyonőrséghez képest jogaik, kötelezettségeik és képzési feltételeik sokkal szigorúbb követelményűek. Szolgálat ellátásuk során viselhetnek és használhatnak lőfegyvert, pórázon és szájkosárral vagy mindkettőt mellőzve kiképzett szolgálati őrkutyát, kényszerítő eszközt alkalmazhatnak a támadó felderítésére és visszatartására. Mindezen cselekvéseket szigorúan szabályozott keretek között végezhetik. Dolgozatom témájának választott fiktív épület azonban nem tartozik az FBŐ alkalmazását indokló objektumok körébe, ezért az őrzésvédelmet polgári vagyonőrség látja el. Az őrzésvédelmi tevékenység végzéséhez a vagyonőrnek és a fegyveres biztonsági őrnek is igazolnia kell egészségügyi alkalmasságát, valamint büntetlen előéletetét az erkölcsi bizonyítvánnyal. [42] [43] [44]

A személy- és vagyonvédelemről szóló törvény értelmében a civil vagyonőr a megbízó felhatalmazásával és nevében jár el munkavégzése során. Figyelemmel kell lennie a környezetében jelentkező anomáliákra, jogsértő tevékenységekre és cselekményekre, illetve azok megelőzésére és elhárítására jelezni és intézkednie kell. A komplex védelmi rendszer nélkülük nem lenne kellő hatékonyságú, hiszen az elektronikai rendszerek nem képesek kiszűrni a gyanúsan viselkedő személyeket, az épület berendezéseiben történt apróbb változtatásokat, a munkavállalók szabálytalan tevékenységét vagy a vagyonvédelmi rendszerfelügyeleti helyiségben a monitorokra kivetített videóanyag riasztást nem kiváltó rendellenességét. Összefoglalva az emberi viselkedés, motiváció értelmezéséhez továbbra is élőerő alkalmazása szükséges. [12] [44]

A mechanikai- és elektronikai rendszerekkel, szervezeti szabályzókkal azonosan a vagyonőri tevékenységnek is keretet kell szabni. Napi munkavégzésüket az őrszolgálati utasításban foglaltaknak megfelelően kell végrehajtaniuk. A szabályzat kiemelt jelentőségű, hiszen a vagyonőrnek pontos ismeretekkel kell rendelkeznie, hogy mikor, mit és hogyan kell elvégeznie, mire kell reagálnia. Ennek hiányában a napi szolgálat kaotikus lenne, ami súlyos incidensek sorozatához vezetne. [42] [44]

Az őrszolgálat minden esetben hivatalos egyenruhát vagy formaruhát visel. Általában munkavédelmi boltokból beszerzett fekete cipőt és nadrágot, fehér inget, nyakkendőt. Ezeken jól látható helyen fel szokták tüntetni a vagyonőrt alkalmazó cég nevét, esetleg a megbízó vállalkozó céges nevét. A ruházat egységes megjelenésével és viselésével a vagyonőr vizuálisan elkülöníthető a többi dolgozótól, magabiztosságot és a biztonság állapotának érzetet közvetíti. Megjelenését, magatartását és beszédstílusát a munkahelyi etikettnek megfelelően kell megválasztania. Utóbbiakat fontosnak tarottam megemlíteni, mivel munkatapasztalatom során is számos alkalommal észleltem, hogy azok bőven hagynak kívánnivalót maguk után. Az objektumokba érkező kiemelt üzleti partnerekkel, vendégekkel történő kapcsolatfelvétel és a normáknak nem megfelelő kommunikáció a cég reputációját negatív irányba terelheti és az őrszolgálattal szembeni panasz kivizsgálása további terheket eredményezhet. A nagyobb multinacionális cégek elsősorban idegen nyelvet is beszélő munkaerőt keresnek, ami a hazai munkaerőviszonylatban igen ritkának számít, ez további kommunikációs problémák gyökéroka lehet. Munkaidejük huszonnégy órában van maximalizálva, ami nyolc vagy tizenkét órás műszakokkal is felváltható. Utóbbiak okán váltásos szolgálati rendszerben működnek, így a törvényileg előírt megfelelő pihenő idő biztosítva van. [12]

4.2. A vagyonvédelem operatív működése

A korábbi fejezetekben azonosított kockázatok, mint például az ipari kémkedés, illetéktelen behatolás, szabotázs és egyéb támadások kizárólag mechanikai és elektronikai jelzőrendszerekkel hatékonyan nem kezelhetőek. Szükség van az őrszolgálat személyes jelenlétére is, ezáltal a műszaki eszközökkel összhangban határozott és gyors döntések, ellenreakciók hajthatóak végre a fenyegetettség megszüntetésére.

A tevékenységüket szabályozó jogszabály előírja, hogy napi munkavégzésüket a szolgálati rend szerint kell végrehajtaniuk. Ennek előzetes kidolgozása és írásban való rögzítése alapvetően a Kft-vel közösen történik annak profiljának-, az objektum adottságainak, jellemzőinek és az azonosított kockázatoknak megfelelően az alábbi területekre és feladatokra összpontosul:

- Beléptetés ellenőrzése, vagyis az érkező és távozó munkavállalók, alvállalkozók, vendégek kontrollja, regisztrációja személyi igazolvány felmutatásával.
- Be- és kihajtó gépjárművek rakterének ellenőrzése.
- Az objektumba behozott mobiltelefonok, laptopok és egyéb kép- és hanganyag rögzítésére szolgáló eszközök regisztrációja, szükség esetén a képrögzítő optika letakarása.
- Járőrözési tevékenység a telekhatár mentén, a parkolóban, az épületen kívül és belül, különös tekintettel a bemutató térre, az adatszobára és a gépészeti helyiségre.
- Védelmi eszközök jelzéseinek a rendszerfelügyeleti helyiségben történő ellenőrzése.
- Tűz esetén a kiürítés segítése, beavatkozó erők értesítése és a riasztási lánc hierarchia szerinti elindítása.
- Testi épség veszélyeztetése nélkül egyéni mérlegelés alapján a tűz oltásának megkezdése, extrém mennyiségű csapadék érkezésekor a víz szabad lefolyási útjának biztosítása a víznyelők felnyitásával.
- Az őrzés során az objektum adottságainak, dolgozói rutinjának ismerete által a szabálytalanságok, károkozásra törekvő szándék felismerése.
- Adminisztráció során a szolgálati dokumentumok pontos, naprakész vezetése.
- Diszpécseri szolgálat.
- Elsősegélynyújtás.

A részletezett feladatok összetettsége is mutatja az élőerős őrzés objektumvédelemben betöltött nélkülözhetetlen szerepét. A várható és váratlan helyzetekre való reagálás, a gyors döntési képesség és a munkavállalók irányába biztonságot jelképező személyes jelenlét kellő felkészültséget igényel. A kritikus és magas kockázati szinttel rendelkező adatszobára, gépészeti helyiségre és bemutató térre megkülönböztetett odafigyelés szükséges, mivel a Kft. esetében ezen helyiségek integritásának károsodása vezethet az üzletmenet folytonosság megakadásához és a piaci szereplőkkel szembeni versenyhátrány elszenvedéséhez. [44] [45]

A szolgálati rend vagy őrszolgálati utasítás pontos információkat kell, hogy tartalmazzon az adott helyzetre történő reagálással kapcsolatban. A hatékony intézkedés megvalósításához szükséges a vagyonőr munkaeszközeit meghatározni, rendszeresíteni és esetlegesen annak alkalmazására betanítani őt. A szabályzatnak tartalmaznia kell a szolgálati hierarchiát, a jelentési kötelezettség tartalmi elemeit és módját, vagyis a szolgálat során az adott esemény kommunikációs eszközzel történő közlését a felettessel. A működési rendben fontos tisztázni, hogy a munkaidejük alatt magán mobiltelefon és internet böngészésre alkalmas egyéb elektronikai szórakoztató eszközt nem tarthat magánál a vagyonőr, mivel az jelentősen hátráltatná vagy meghiúsítaná a hatékony szolgálatellátást például a külső vagy belső támadás alatt értendő behatolási szándékot, adat- is információszerzésre tett kísérletet, rongálást, szabotázst, gépjármű feltörést, stb. Ezen szabályok betartásához és betartatásához elemi érdeke fűződik a Kft.-nek és a megbízott vagyonőri vállalkozásnak. [42] [45]

Az operatív működés során szintúgy kiemelt figyelem fordítandó a beléptetés ellenőrzött keretek között tartására. A kritikus kockázattal érintett helyiségek miatt eltérő belépési jogosultságokkal fognak a dolgozók rendelkezni. Ennek megszervezése és megfelelő kiosztása, beállítása a belépő kártyákkal kerül megvalósításra. A kártya azonosítási technológiáját kezelni tudó kártyaolvasót a beléptető kapun kell elhelyezni. A 7. ábrán háromkarú forgóvillás beléptető megoldás látható. A zónaszinteknek megfelelő hozzáférések kezelési folyamatát azonban nem végezheti a vagyonőri szolgálat vállalatbiztonsági okoknál fogva, csak az adott személy hozzáférését ellenőrizheti például a kártyára ragasztandó védelmi zónaszint jelölését szolgáló matrica által. Utóbbi megoldással lehet élni a bemutató tér esetében is. A kiállított eszközök folyamatos váltakozása során előfordulhat, hogy időszakonként engedélyezett a kép- és hanganyag készítése. Ilyenkor a használandó eszközt előzetesen regisztrálni kell és a belépő kártyára hasonló matrica felragasztása szükséges például „Rögzítés engedélyezett” felirattal és piktogramokkal. [45]

7. ábra: Háromkarú forgóvillás beléptető kapu [46]

A belső támadások elkövetése megvalósulhat az őrszolgálat által is. Ennek megelőzésére kötelező a napi szolgálati csoport vezetőjének véletlenszerű bejárásokat, ellenőrzéseket tartania, így kontroll alatt tarhatja a beosztottjait. A humán jellegű kockázatokra adott válaszok, vagyis az oktatás és érzékenyítés a vagyonőröknél is releváns támpontot ad. Előbbiek nem lehet kellőképpen hangsúlyozni, hiszen átvitt értelemben a védelem első (emberi) vonalát az őrök képviselik. A támadók megkörnyékezhetik és korrumpálhatják őket. Tekintettel arra, hogy a biztonsági személyzet szenzitív adatokat is kezel, ezért könnyen adatszivárgással és személyiségi jogokkal való visszaéléssel vádolhatóak meg. [42]

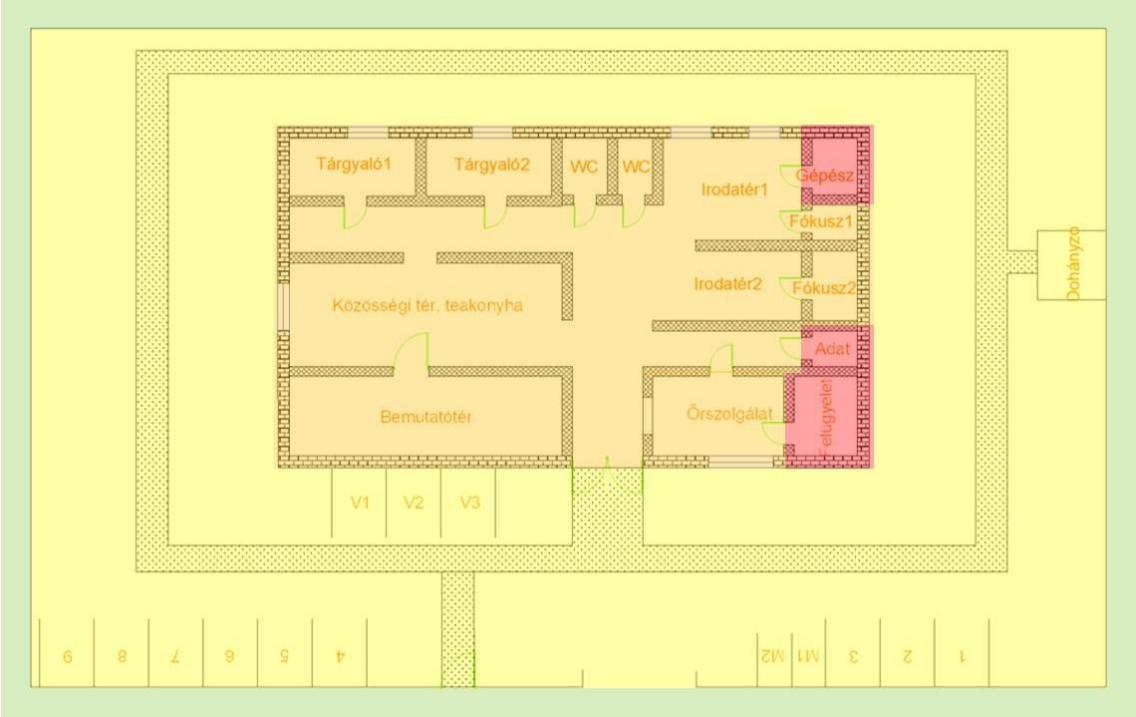
4.2.1. A vagyonőrök szolgálatszervezése

Az őrszolgálati utasításban foglalt feladatokat különböző pozíciót betöltő őrök látják el. A Kft. esetében kizárólag megfelelő képesítéssel rendelkező vagyonőrök alkalmazása valósul meg, ezért a szolgálatban levő személyzet minden tagjának részt kell vennie a beléptetés ellenőrzésében, a járőrözésben, a portaszolgálati teendőkben, dokumentálásban és a rendszerfelügyeleti helyiségben történő felügyeleti, ellenőrzési és jelzési (együttesen operátori) tevékenységben. A napi feladatellátás koordinálását a szolgálat vezető vezényli. A szolgálatszervezés során ügyelni kell arra, hogy a havi beosztás szerint minden napra feltöltésre kerüljenek a pozíciók. Betegség, szabadság vagy egyéb távollétet generáló esemény miatt a vagyonőrzést ellátó vállalkozásnak pótolnia

kell a hiányzó létszámot. A napi szolgálatot adó létszám egy szolgálatvezetőből, egy biztonsági operátorból és egy portaszolgálatos személyből kell állnia. A munkaidő beosztás szerint kettő darab huszonnégyóra- és egy darab nyolc óra folyamatos szolgálatot adó vagyonőrnek kell egyszerre az objektumban tartózkodnia. A jogszabályoknak megfelelően az előbbi esetében a munkavégzést követően negyvennyolc óra pihenési időt kell biztosítani, ezért a Kft. élőerős őrzése három váltásos rendszerben működik. [12] [42] [45]

A beosztás szerint a portaszolgálatot egy fő végzi. Feladata a dolgozók, vendégek fogadása és szükség esetén hivatalos személyi okmány felmutatásával történő regisztrációja, vendégkártyák kiadása, a portára érkező telefonhívások megválaszolása. Rendezvény megtartása alkalmával a kíséret biztosításának okán a napi létszám bővítésre szorulhat, melyről előzetesen gondoskodni kell. Ügyel a gyanús személyekre és az épületbe bevinni szándékozott illetéktelen tárgyak kiszűrésére.

A járőrözési útvonalak bejárását a napi szolgálatszervezési dokumentumban előre meghatározott, de véletlenszerű és soha nem ismétlődő időpontokban végzik. A feladatot folyamatos jelleggel, pozícióváltásokkal kell végrehajtaniuk. A nullától harmadik szintig kialakított védelmi zónarendszert bejárás során szemrevételezni kell, különös tekintettel a kritikus kockázattal érintett helyiségekre és egyéb nem szokványos helyzetekre, állapotokra. A kockázati szinteknek megfelelő zónabesorolás színekkel történő vizuális megjelenítését a 8. ábra szemlélteti. A járőrözés során az objektum jellemzőit figyelembe véve különböző helyiségeknél és telekhatár menti területeknél őrjárat ellenőrző pontok kialakítása szükséges. Ezeket a bejárás elvégzésének igazolására kell használni a vagyonőr RFID kártyájának vagy bilétájának leolvastatásával. A sikeres azonosítás rögtön naplózásra kerül. [7] [45]



8. ábra: Az objektum védelmi zónaszintjei [Saját kép]

A rendszerfelügyeleti helyiségben egyszerre kettő fő vagyonőr látja el szolgálatát huszonnégy órás ügyeleti rendszerben, ezáltal az objektum éjszakai biztosítása is megoldott. A pozíció értelmezése szerint ellátják az épület sarokpontjaihoz telepített és egymásra rálátó CCTV kamerarendszer által átjátszott videóanyag felügyeletét és elemzését. Figyelemmel kísérik a sorompó, a mozgásérzékelő, a meteorológiai figyelő rendszer jelzéseit, melyet a 9. ábra szemléltet. Mindezen tevékenységek megosztott figyelmet igényelnek, ezért a két fő összehangolt munkája elengedhetetlen. A korábban említetteknek megfelelően – az előre nem látható okok miatti szolgálati létszámhiány megoldására – a szolgálatszervezésben gondot kell fordítani a helyettesítés rendelkezésre állásának biztosítására is. A gyakorlati megoldás szerint a vagyonvédelmet ellátó vállalkozásnak az előre meghatározott és vagyonőrökkel feltöltött készenléti állomány bevonásával vagy kötelezően elrendelt túlórával kell garantálni a felügyelet fenntartását. [42]

9. ábra: Operatőr a rendszerfelügyeleti helyiségben [47]

4.2.2. A vagyonőrzési adminisztráció és kommunikáció

A vagyonvédelmi ágazatban kiemelt jelentőségű a pontos, részletes időadatokat, esemény- és intézkedési leírásokat tartalmazó szolgálati dokumentációk létrehozása. Ezáltal az adott incidens, például emberi mulasztásból fakadóan nyitva hagyott biztonsági ajtó vagy illetéktelen tartózkodás a jogosultságnál magasabb zónaszintben könnyen visszakövethető és mind a vagyonőr, mind a cég érdekeit védi jogi szempontból. [12]

A fiktív objektum esetében a Kft. törekszik a digitalizáció által nyújtott lehetőségek kiaknázására, vagyis a belépési időadatok, a munkaidő nyilvántartás, az objektumvédelem során a rendszerek által generált jelzések elektronikus naplózására, valamint a biztonsági eseményekről készült jegyzőkönyvek készítésére. Azonban a mai napig is van létjogosultsága bizonyos esetekben a papíralapú nyilvántartások vezetésének. A vagyonőrzés során mindkét módszer alkalmazásra kerül példának okáért a mozgásérzékelő riasztási jelzéseinek rögzítésénél vagy a szolgálat felvétel- és leadás alkalmával. A védelmi rendszerekben keletkező esetleges anomáliák során továbbra is

meghatározó szerepet játszik az emberi ítélő- és döntőképesség, melyek fizikális rögzítése nélkülözhetetlen. [42] [45]
A vagyonőrzési tevékenységhez hozzátartozik a tömör, lényeget közlő kommunikáció, ami elsődlegesen szóban, másodlagosan a rádióforgalmazást használó rendszeresített adó- és vevőegységekkel történik. Szolgálati mobiltelefonnal csak a szolgálatvezető rendelkezik. A gyors és egyértelmű jelzés, továbbá a felettesnek való azonnali jelentési kötelezettség teljesítése szignifikánsan lecsökkenti a reagálási időt, ennek gyakoroltatása a beosztottakkal fontos tényező. [45]

A fentebb részletezett tevékenységek minősége, vagyis az adott napon megvalósult események kommunikációja és dokumentálása a munkaidő végén, azaz a szolgálat átadás-átvételkor is azonos súlyponttal rendelkeznek. A szabályoknak megfelelő feladatellátás és annak közlése, átadása a következő napi szolgálatnak kiemelt jelentőségű, hiszen ezek ellenében diszfunkció keletkezhet. [42]

A fejezetben bemutattam a vagyonőrzés szerepét, törvény biztosította működési feltételeit és feladatait az objektumvédelemben. A mechanikai védelem és elektronikai jelzőrendszerek melletti harmadik tényezőként a jelenkori felgyorsult világban továbbra is kulcsfontosságú szerepet töltenek be a komplex vagyonbiztonságban. A következő fejezetben a rendszerek együttes működését és a hozzá kapcsolódó incidenskezelést mutatom be.

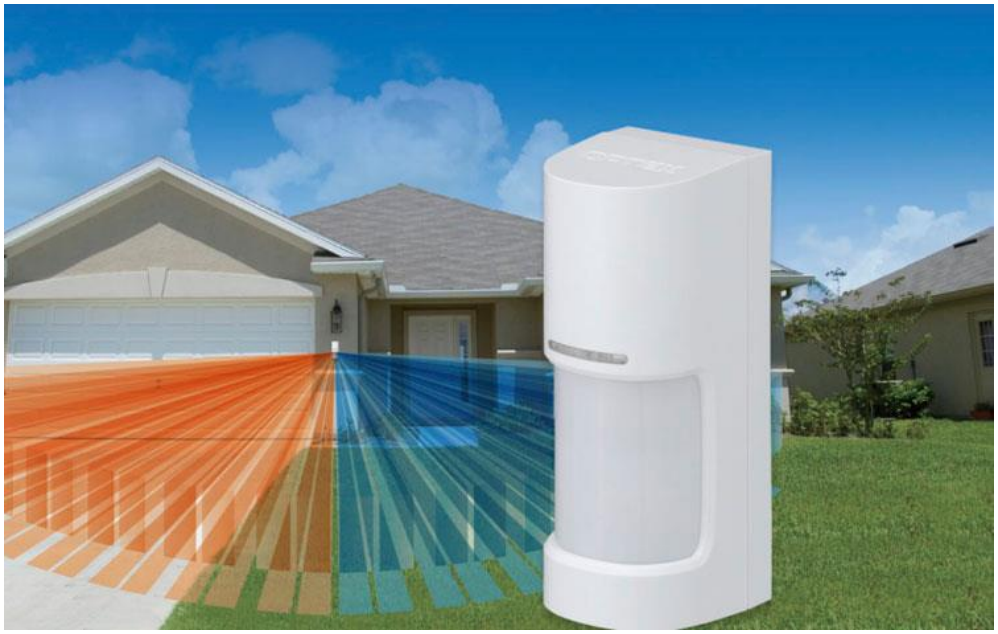
5. KOMPLEX BIZTONSÁGI RENDSZER MŰKÖDÉSE ÉS INCIDENSKEZELÉSI PROTOKOLLOK

Az előző fejezetekben bemutattam a védendő objektumot, annak jellemzőit és a tulajdonosi cég profilját. Az épület elhelyezkedése és a Kft. tevékenységi köre okán alacsony és kritikus kockázati tényezőkkel is számolni kell, melyek azonosítását követően biztonságtechnikai javaslatokkal éltem. A rendszer különálló elemeiként funkcionálva a védelmi tervezés hiábavaló volt. A telepített eszközök és megoldások csak akkor képeznek komplex vagyonvédelmi rendszert, ha működésük összehangolása és finomítása megtörtént, illetve folyamatos felügyelet alatt állnak. Dolgozatom ezen részében a személy- és vagyonvédelem során alkalmazandó komplex és integrált objektumvédelmi eszközöket egységes rendszerben való kezelését és működését, valamint a biztonsági eseményre történő reagálási és riasztási láncot mutatom be. [34]

5.1. A komplex védelem felépítése

Az objektumot védeni hivatott rendszer kialakításának első lépéseként meghatároztam, hogy az adott fenyegetettségre milyen típusú eszköz telepítése, beépítése javasolt. A tervezés célja és elsődleges feladata az elrettentés és a további incidensek időbeni késleltetése. Ezek alapján a mechanikai védelmet a telekhatárt kerítéssel, forgóvillás beléptető kapuval, automata működésű szakállas sorompóval és tolókapuval határolja le. Az objektum külső határa és az épület között mozgásérzékelők telepítését javasoltam, mely tovább növeli a mélységi védelem hatékonyságát, amit a 10. ábra jelenít meg vizuálisan. Az eszköz által biztosított területre behatoló személyt detektálja és riasztást ad le a központnak. Az épület nyílászáróinak biztonsági fóliázása növeli az üvegfelületek ütéselnyelését és megnehezíti az épületbe való bejutást. A létesítmény portaszolgálati pultját követő helyiségekbe történő bejutás határvonalánál a kettes zónaszintnek megfelelően szintén beléptető kapu alkalmazása szükségszerű a bemutató tér bejáratához hasonlóan. A harmadik védelmi zónába eső adatszobát, gépészeti helyiséget és rendszerfelügyeleti helyiséget kritikus kockázati besorolásának köszönhetően biztonsági

ajtókkal, normál vagy fordított működésű zárrendszerrel, belépési jogosultságot szabályozó RFID kártyaolvasóval kell felszerelni. [34]



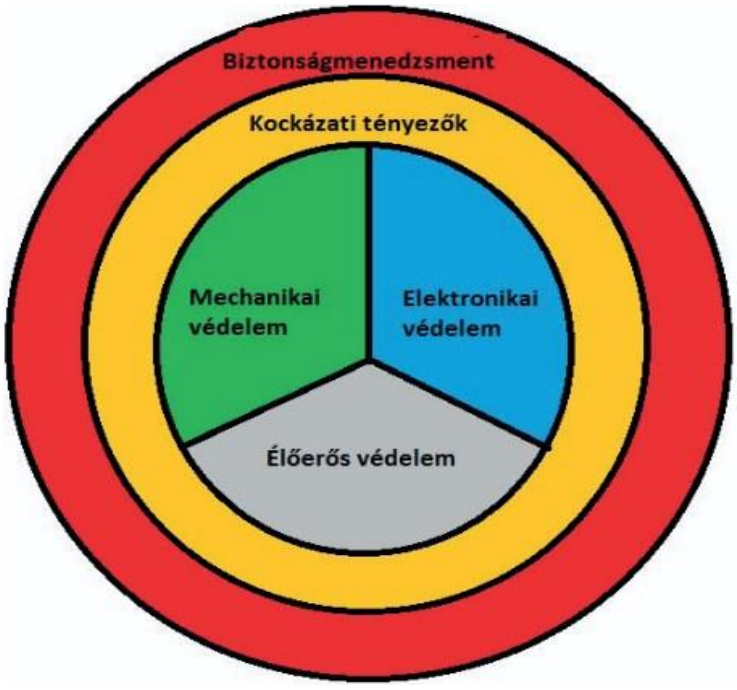
10. ábra: Mozgásérzékelő jelzőrendszer [48]

Az elektronikus jelzőrendszer célja, hogy a mechanikai akadályt leküzdő támadó észleléséről jelzést adjon a beavatkozást végrehajtó őrszolgálatnak. Ezáltal a vagyonőri reagálási folyamat jelentős mértékben csökken, hiszen a rendszerfelügyeleti helyiségből akár a kamerafelvételeken előre is látni lehet a fenyegetést. A CCTV kamerarendszer, mozgásérzékelők, RFID kártyaolvasók fejlődésük révén már digitális IP-alapú (Internet Protocol, magyarul internetprotokoll) kommunikációt használhatnak és közvetlenül a felügyeleti rendszerbe továbbíthatják az adatokat, így azok naplózhatóak és később is elemezhetőek, illetve több jelzés esetén prioritási sorrend állítható fel. A tűzvédelmi berendezéseket tekintve a tűzjelzők, hő- és füstérzékelők, automatikus oltórendszerek, kézi tűzjelzésadók szintén külön dedikált tűzjelző központban kerülhetnek összefogásra, azonban nem IP-alapon. A kiépített komplex rendszertől napjainkban elvárható, hogy működése során minden jelzőrendszer képes legyen a számára meghatározott központba irányítani az információkat. [34] [8]

Az élőerő az objektumvédelem harmadik alappilére és egyben a komplex rendszer kiemelt részegysége. Megjelenésükkel és szolgálat ellátási feladataikkal visszatartó erőt képviselnek a támadókkal szemben, ugyanakkor a Kft. munkavállalóiban is

biztonságérzetet keltenek. Az objektum integritását folyamatosan monitorozza, járőrözést hajt végre, kezeli és felügyeli a céghez érkező személyeket, gépjárműveket, kiszűri a gyanús viselkedést, összességében reagál az incidensek megelőzésére, elhárítására és a károk minimalizálására. Munkájukat nagymértékben segíti a megfelelő tervezést követően kialakult mélységi- vagy héjvédelem. [44]

A komplex vagyonvédelem kialakítása rendszerekben való gondolkozást jelent. A mechanikai védelem, elektronikai jelzőrendszerek, élőerős őrzés, valamint a szervezeti és vállalati szabályzók kulcsfontosságú elemei, melyet a 11. ábra szemléltet. A kockázatoknak megfelelő védelmi zónarendszer kialakításával pontosan meghatározható azon optimális eszközpark és intézkedési terv, ami a fenyegetettség kontroll alatt tartásához, megelőzéséhez, késleltetéséhez kell. A Kft. esetében a biztonsági szinteket meghatároztam, így a cég vezetőségén múlik, hogy a kockázatokat elfogadja, csökkenti, kerüli vagy megosztja.



11. ábra: A komplex védelem [49]

A védelem egységeinek sérülésével láncreakció indulhat el, ezáltal az objektum integritásában zavar keletkezhet. Váratlan meghibásodás esetén szükséges lehet az őrszolgálat személyi létszámának megemelése és járőrözési tervének kibővítése, áramkimaradás esetén az elektronikus naplózás papíralapúra történő módosítása.

Mindezen védelmet tovább lehet fokozni az alrendszerek integrálásával. Ez a gyakorlatban a komplex védelem összehangolását és kapcsolódását jelenti a kommunikációs jelzések megvalósulásával és az egységes felügyeleti rendszerrel. [8] [50]

5.2. Az integrált vagyonvédelem

A modern objektumvédelmi rendszerek fejlődési iránya egyértelműen az integrálható eszközök számának és technológiai fejlettségének irányába halad, melynek célja a rendszerek egymást támogató funkciójának bővítése. A tervezés során a védelmi eszközök kiválasztásának szempontja, hogy rendszerbe foglalásuk eredményeként a közös felügyeleti központon keresztül történjen az operátor általi monitorozásuk, kezelésük. Az integrált vagyonvédelem nem valósulhat meg az alapvető egységeit jelentő fizikai eszköz (hardver) és annak irányítását kezelő program (szoftver) nélkül. Ez a gyakorlatban azt jelenti, hogy a rendszerfelügyeleti helyiségben elhelyezett asztali számítógépbe futnak be a jelek, amit a gyártó által programozott szoftver segítségével jelenítünk meg monitorokon, televíziókon. Fontos megjegyezni, hogy a gyártók a saját fejlesztésű alkalmazásaikat részesítik előnyben, ezért az eltérő eszközök nem minden esetben tudnak kommunikálni egymással. A különböző jelzőrendszerek központjai alap esetben nem állnak összeköttetésben a központi felügyelettel. Példának okáért tűzvédelmi vonatkozásban a tűzjelző központba fut be minden tűzzel kapcsolatos jelzés, de ezen kívül a kézi jelzésadó a vagyonvédelem központi felügyeleti részét is képezheti, ezáltal tűzjelzés esetén a beléptető kapuk tűzeseti vezérlése megvalósulhat a forgóvillák átengedő mechanikáinak deaktiválási funkciójával. A rendszerek hardveres és szoftveres részeinek kiválasztása szakmai tapasztalatot és körültekintést igényel. [2] [34]

Az objektum védelmének aspektusából a mechanikai védelem, vagyis a kerítés, biztonsági ajtók, zárszerkezetek, beléptetési kapuk fizikai akadályt támasztanak a behatolóval szemben. Hatékony működésükkel elérhetővé teszik a jelzőrendszerek számára a támadó detektálását például a térfigyelő kamerák által. A 12. ábra a kerítés és a kamera együttes alkalmazását szemlélteti. A beléptetési rendszerrel kiegészített

biztonsági ajtók és kapuk összeköttetésben állnak a felügyeleti rendszerrel, így a jogosulatlan belépési szándékot valós időben jelzik az őrszolgálat részére. [34]

12. ábra: Elektronikai jelzőrendszer által megfigyel mechanikai védelem [51]

Az elektronikai jelzőrendszerek képezik a védelem legérzékenyebb pontját több szempontból is. A Kft. esetében az objektum elhelyezkedése, működése és arányos védelmének kialakítása okán nem javasoltam a mozgásérzékelőn kívül egyéb jelző eszközt, de a piacon számos alternatíva érhető el. A teljesség igénye nélkül: nyitás-, törés-, jelenlét-, hang alapú érzékelők vagy hőmérséklet és páratartalom figyelő rendszerek. Ezeket behatolásjelző rendszereknek is nevezhetjük és jelzéseiket a felügyeleti központba küldik tovább. A rendszerben keletkező anomália felboríthatja és megbéníthatja a riasztási láncolatot például fals adatok küldésével. További problémát okozhat, ha a jelzések továbbítása átjelzéssel valósul meg és a távfelügyelet ellátó külsős vállalkozás részére kerül átküldésre. Az ilyen esetek megoldása sok dolgozó idejét leköti mire a gyökérok meghatározásra kerül, illetve a hiba elhárításáig ideiglenesen bevezetett intézkedések szükségtelen terhet rónak a cég működésére. [34] [8]

A zártláncú televíziós- és beléptető rendszer összekapcsolása is fontos szempont az integrált vagyonvédelemben. A kamerák által átjátszott képi anyag lehetővé teszi az incidens élőerő általi verifikációját, mely döntéselőkészítő funkcióval bír. Gyakorlati

példával élve a Kft. telekhatáránál illetéktelen behatolási vagy jogosultság hiányából fakadó belépés megtagadási eseményeiről az őrség valós időben értesülhet, így az intézkedés megtételét azonnal elkezdheti. Ezen technológia megoldást az analitika fejlődése hozta magával, azonban a nem megfelelő beállítások indokolatlan jelzések sokaságát generálhatják. Hasonlóan a mozgás- vagy egyéb érzékelővel való integrálához. Az érzékelő jelzésére a kamera az adott irányba fordulhat el vagy optikai közelítéssel vizsgálhatja a területet. Ennek rossz paraméterezése az üzemszerűen megfigyelt terület feletti kontroll elvesztésével járhat, illetve kettő vagy több támadó esetén kijátszhatóvá válhat. Az utóbbi működtetésbeli anomáliákat leszámítva összességében a kamera és a beléptető rendszer együttes alkalmazása a védelem hatékonyságát jelentősen növeli. [34] [8]

Az alrendszerek összefogását a felügyeleti szoftver végzi el, így kiemelt jelentőséggel bír a felhasználóbarát platformjának kialakítása. Lényege, hogy a fogadott jelzéseket egyidejűleg, akár több monitoron is képes legyen megjeleníteni. Az adatok megjelenítése jelzésenként vagy összefoglalva is megjelenhet. Fontos, hogy az adott jelzéshez pontosan meghatározza az azt leadó készülékegységet, helyét vagy kódszámát és a jelzést kiváltó időpontot. Több jelzés egyidejű befutása esetén a felprogramozás során megadott kritériumok szerint kell priorizálnia, vagyis a magasabb kockázati értékű jelzést kell előrébb sorolnia a kép megjelenítőn. Gyakorlati megközelítésben az egyik munkavállaló éppen a kerítésmenti belépő kapunál nem találja a kártyáját és fizikális erőt fejt ki az átengedő szerkezetre. Eközben a parkolóban egy másik dolgozó a gépjárművek utastereinek tulajdonít megkülönböztetett figyelmet és az ajtónyitó szerkezetek zárt állapotát vizsgálja. Mindezekkel egyidőben a felügyeleti rendszerre jelzés érkezik az adatszoba beléptetési kártyaolvasója által a többszöri jogosulatlan belépési szándékról. A rendszerfelügyeletet éppen ellátó operátor monitorján a három eset a kockázati szintnek megfelelő sorrendben jelenik meg, vagyis először a kritikus zónaszint megsértésének kísérlete, a magas besorolású gépjármű feltörés, majd a közepes kockázatú gyanús viselkedés.

Ezen esetek is alátámasztják a vagyonőri jelentlét szükségességét. A felügyeleti monitoron priorizált sorrendben megjelenített eseményeknél dönthet úgy az őr, hogy az első kettő incidens elhárítását követően a telekhatármenti belépési pontnál kártyáját

kereső személy gyanúja már többször előfordult és pár másodpercen belül mindig előkerül a belépőkártya, tehát az azonnali intézkedés nem indokolt. [8] [44]

Fontos megemlíteni, hogy az adatszobához használt szünetmentes tápegységhez hasonlóan az integrált rendszerek átmeneti áramforrásáról, vagyis a redundancia biztosításáról is gondoskodni kell. Az aggregátor használata a Kft. objektumában nem életszerű, ehelyett akkumulátorok beszerzése indokolt. Utóbbiak használata minden jelzőrendszer esetében szükséges. Amennyiben az integrált rendszer egyik eleme, például a CCTV kamera meghibásodik és a mozgásérzékelő rendszer áramszünet miatt nem képes az észlelésre, úgy rögtön két eszköz esik ki a védelem ellátásából. [2] [34]

Az integrált vagyonvédelmi rendszer összetett folyamatok összessége. Minden eleme meghatározott helyet és szerepet tölt be a védelmi ellentevékenységen belül. A folyamatos karbantartás, szoftver frissítések telepítése és az élőerő bevonásával történő gyakorlatok végrehajtása elengedhetetlen. Megfelelő szervezés és működés esetén az objektum integritása biztosított lesz.

5.3. Az incidenskezelési protokoll

A komplex és integrált vagyonvédelmi rendszer működésbeli teljes hatékonyságát abban az esetben éri el, ha képessé válik a biztonsági eseményekre gyorsan, precízen reagálni. A protokoll olyan folyamat, mely előre meghatározott válaszreakciókat foglal magában. Pontosan - a köznyelvben csak ki-mit-hol-miért-hogyan és minek a segítségével kérdéseket - leszabályozó intézkedési csoportok. Az incidenskezelés során az ellentevékenységet végrehajtó személy információval rendelkezik arról, hogy a bekövetkező biztonsági esemény milyen kockázati kategóriába tartozik és melyik védelmi zónaszintet érinti. Ezek alapján kezdi meg a támadás elhárítását vagy a szükséges tevékenységet. [33] [44]

Az incidenskezelési- vagy biztonsági eseménykezelő protokoll (‚másképpen intézkedési terv) elkészítése során ügyelni kell arra, hogy az objektumvédelem során alkalmazandó eszközöket, szervezeti szabályzókat, vagyonőri utasítást és minden egyéb a védekezéssel

összefüggő információt tartalmazzon. Az őrzést végrehajtó biztonsági személyzet szabályzataihoz hasonló reagálási terv, azonban tartalmaznia kell a megbízó vállalat felsőbb szintű jelentési és beavatkozási eseménysorát is. Az intézkedési terv többlépcsős felépítésű, egymásból következő és épülő cselekvések sorozata. A protokoll lényegét a következők szerint lehet összefoglalni: az emberi életet és a Kft. javait veszélyeztető események esetén mindazon intézkedések, cselekvések, felelősségi körök, jogok és kötelezettségek meghatározása, továbbá a védelem során alkalmazott eszközök és beavatkozó személyek összessége, melyekkel a veszélyeztetettség elhárítható, megszüntethető, késleltethető és az okozott hatás csökkenthető, figyelembe véve a jogszabály adta keretek és a Kft. belső szabályzatait. [33] [44]

A tervnek a meghatározott intézkedési folyamat szerint kell végrehajtásra kerülnie. A védendő fiktív objektumra levetítve az incidenskezelési protokollt a következő eljárás rend szerint kell teljesíteni: észlelés, incidens verifikálás, reagálás, riasztási lánc elindítás, dokumentálás, incidens és reagálás elemzése. A folyamatlépések elvégzése elsődlegesen a vagyonőri szolgálat feladatkörébe tartozik. A felsorolt lépéseket külön nem részletezem, mivel dolgozatom korábbi fejezeteiben már megtettem és azok újbóli ismétlését nem tartom indokoltnak. Ellenben jelen bekezdésben fontosnak tartom kiemelni a riasztási láncolatot. Elindításán belül a szolgálatvezetőnek történő jelentési kötelezettség a biztonsági esemény fajtájától függően időben eltérhet, de folyamatosan végezni kell. A jelentési kötelezettség elmulasztását indokolhatja olyan veszélyhelyzet kialakulása, amikor nincs vagy csak kevés idő áll a vagyonőr rendelkezésére és mérlegelnie kell a szolgálati út betartása és az incidens (például életmentés, tűz eloltása, stb.) megoldása között. [33] [44]

Kiemelendő, hogy a protokoll nem kizárólag a vagyonőri teendőket tartalmazhatja. Vonatkozhat a vállalat belső embereire külön és a vagyonőri szolgálattal egybevonva is. Elkészítése szintén rendkívül fontos és hatással van a cég hatékony működésére. Utóbbi esetnél maradva a vagyonőri utasításban foglaltakon felül a szolgálatvezető a Kft. által megbízott belsős kapcsolattartón keresztül kommunikált. Ez a személy általában biztonságtechnikai- tűzvédelmi- vagy EHS (jelentése Environment, Health, Safety, magyarul megfelelője környezet-, tűz- és munkavédelmi szakember) mérnök. A Kft.

képviseletében eljáró személynek szintén jelentési kötelezettsége áll fenn például a vállalatbiztonsági vezető részére, aki szintén tovább jelent a felsővezetés számára. A kialakított hierarchia alapján a felelősségi körök egyértelműen leszabályozottak, betartásukkal az incidensek kezelhetővé válnak. [33] [44]

A fejezetben bemutattam a komplex és az integrált vagyonvédelem kialakításának elvi rendszerét és működését. Gyakorlati példákkal szemléltettem az objektumvédelem három pillérét adó mechanikai védelem, elektronikai jelzőrendszer és élőerős őrzés összehangoltságát, az incidensekre adott ellentevékenységekre fókuszálva. Végül az incidenskezelési protokoll szerepét taglaltam általános megközelítéssel. A biztonságtechnikai eszközökhöz hasonlóan az intézkedési terveket is számos nemzetközi szabvány támogatja, melyek nem képezik részét dolgozatomnak.

ÖSSZEGZÉS

A dolgozatom célja az objektumvédelem bemutatása volt egy elképzelt cégen és objektumon keresztül, valamint a kiépítendő optimális és arányos védelem koncepció tervének elkészítése. Ennek során javaslatokat fogalmaztam meg a biztonságtechnika, mint tudomány által biztosított információk, kutatások és eszközök útján. A munkám során szeretem a komplex dolgokat távolról megközelíteni, majd részletekbe menően elemezni, ez indokolja a témaválasztásomat.

Az első fejezet során taglaltam az objektumvédelem elméleti rendszerét, vagyis külön-külön az őrzés, a védelem, az objektumvédelem fogalmi meghatározásait és a vonatkozó jogszabályokat. Ezt követően részletesen bemutattam a megbízómat, vagyis a FutureAi Kft. elnevezésű fiktív céget, annak profilját, az objektumának részét képező épület környezeti és belső adottságait. Elvégeztem a létesítmény szemszögéből felmerülő kockázati események azonosítását, elemzését, melyek ábrázolására kockázati mátrixot készítettem el. A biztonsági események valószínűségének és hatásának figyelembevételével konkrét védelmi eszköztípusokat javasoltam. A negyedik egységben kitértem az objektumvédelem kötelező részét képező élőerős őrzést végrehajtó vagyonőri szolgálatra, annak működési feltételeire, szabályaira. A záró fejezetben értekeztem a komplex és integrált vagyonvédelemről, incidenskezelési protokollról és igyekeztem azokat gyakorlati példákkal szemléletesebbé tenni.

A dolgozat megírásának folyamata közben számos forrást gyűjtöttem és elemeztem. A témám kutatása során jelentősen eltérő szakterületekkel találkoztam, melyek tovább erősítik a biztonságtudomány interdiszciplinaritását. A mai felgyorsult világban nehéz lépést tartani az új technológiák, főleg a mesterséges intelligencia fejlődésével. Véleményem szerint a közeli jövőben az innovációk meghatározó irányává válik, illetve már most is annak tekinthető. A digitalizáció nyújtotta lehetőségek hazai viszonylatban való erősebb megjelenésének felgyorsítása és munkavállalói használatának ösztönzése kiemelt jelentőséggel bír a globális versenypiac által szabott feltételeknek való megfelelés és felzárkózás tekintetében.

A geopolitika alakulásából is következőn az MI mellett a dróntechnológia elterjedését látom a másik meghatározó csapásiránynak. A kettő összehangolása jelenleg is zajlik és érdeklődéssel tekintek az új technológiák megjelenése felé. A biztonságtechnikát, azon belül a vagyonvédelmet illetően az RFID kártyákat hamarosan felváltó NFC- és a későbbiekben a biometrikus alapú megoldások megjelenését várom kíváncsisággal, illetve ezek vagyonvédelembe történő átültetési megoldásait.

Munkám végzése során sokszor tapasztalok hanyag hozzáállást a munkavállalók részéről, ezért a cégek vagyonvédelmének fejlesztési potenciálját a korábban említetteken kívül a dolgozók oktatásának minőségi javításában és érzékenyítési kampányok szervezésében látom.

SUMMARY

The aim of my thesis was to present object protection through an imaginary company and object, as well as to plan the optimal and proportionate protection to be developed. In doing so, I made recommendations based on information, research, and tools provided by security technology as a science. In my work, I like to approach complex issues from a distance and then analyze them in detail, which explains my choice of topic.

In the first chapter, I discussed the theoretical system of property protection, i.e., the conceptual definitions of guarding, protection, and property protection, as well as the relevant legislation. I then presented my client, a fictional company called FutureAi Kft., in detail, including its profile and the environmental and internal characteristics of the building that forms part of its property. I identified and analyzed the risk events arising from the perspective of the facility, which I illustrated using a risk matrix. Taking into account the probability and impact of security incidents, I recommended specific types of protective measures. In the fourth unit, I discussed the security guard service that provides manned security, which is a mandatory part of property protection, as well as its operating conditions and rules. In the concluding chapter, I discussed complex and integrated property protection and incident management protocols, and I tried to make them more understandable with practical examples.

During the process of writing this thesis, I collected and analyzed numerous sources. While researching my topic, I encountered significantly different fields of expertise, which further reinforce the interdisciplinary nature of security science. In today's fast-paced world, it is difficult to keep up with new technologies, especially the development of artificial intelligence. In my opinion, it will become the dominant direction of innovation in the near future, and can already be considered as such. Accelerating the stronger emergence of the opportunities offered by digitalization in the domestic context and encouraging its use by employees is of paramount importance in terms of meeting the conditions set by the global competitive market and catching up. Following developments in geopolitics, I see the spread of drone technology as another key trend alongside AI. The coordination of the two is currently underway, and I am looking

forward to the emergence of new technologies with interest. In terms of security technology, and specifically property protection, I am eagerly awaiting the emergence of NFC, which will soon replace RFID cards, and later biometric-based solutions, as well as their application in property protection.

In my work, I often encounter a negligent attitude on the part of employees, which is why I believe that, in addition to the measures mentioned above, the potential for improving asset protection in companies lies in improving the quality of employee training and organizing awareness campaigns.

HIVATKOZÁSOK

[1] Z. Kuris, „A biztonságtechnika tudományszak tárgya és eredményei,” *Hadmérnök,* pp. 39-49, 2010. V. évf. 1. sz..

[2] L. Dr. Berek, Biztonságtechnika, Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[3] L. Tóth, „A komplex objektumvédelem kihívásai napjainkban,” *Bolyai Szemle,* pp. 35-44, 2018/1.

[4] L. Dr. Berek, T. Dr. Berek és L. Berek, Személy- és vagyonbiztonság, Budapest: Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2016.

[5] L. Szabó, Az objektumok biztonsága és az objektumvédelem speciális területe a megelőző védelem, Budapest: Óbudai Egyetem Biztonságtudományi Iskola, 2021.

[6] Z. Jurás, Az elektronikus vagyonvédelmi eszközök aktivitás fokozásának lehetőségei, Budapest: Óbudai Egyetem Biztonságtudományi Doktor Iskola, 2023.

[7] A. Tóth és L. Tóth, Biztonságtechnika, Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[8] Z. Jurás, Tágabb értelemben vett elektronikai vagyonvédelmi ezközök aktivitás fokozásának lehetőségei, Budapest: Óbudai Egyetem Biztonságtudományi Doktori Iskola, 2023.

[9] M. B. Szövetsége, „Betöréses lopás- és rablásbiztosítás technikai feltételei (ajánlás),” [Online]. Available: https://www.pluto.hu/_A/A2.html. [Hozzáférés dátuma: 2025.11.04.].

[10] Belügyminisztérium, „BSR Bűnügyi Statisztikai Rendszer,” [Online]. Available: https://bsr.bm.hu/. [Hozzáférés dátuma: 2025.11.02.].

[11] T. Horváth, Elektronikus megfigyelő-, és ellenőrző rendszerek objektumorientált kialakítása különös tekintettel a biztonsági kockázatok rendszerére, Budapest: Óbudai Egyetem Biztonságtudományi Doktori Iskola, 2018.

[12] „2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól,” [Online]. Available: https://njt.hu/jogszabaly/2005-133-00-00. [Hozzáférés dátuma: 2025.11.03.].

[13] „22/2006. (IV. 25.) BM rendelet a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény végrehajtásáról,” [Online]. Available: https://njt.hu/jogszabaly/2006-22-20-0A. [Hozzáférés dátuma: 2025.11.04.].

[14] „1994. évi XXXIV. törvény a Rendőrségről,” [Online]. Available: https://njt.hu/jogszabaly/1994-34-00-00. [Hozzáférés dátuma: 2025.11.04.].

[15] „27/1998. (VI. 10.) BM rendelet a fegyveres biztonsági őrség Működési és Szolgálati Szabályzatának kiadásáról,” [Online]. Available: https://njt.hu/jogszabaly/1998-27-20-0A. [Hozzáférés dátuma: 2025.11.04.].

[16] „2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről,” [Online]. Available: https://njt.hu/jogszabaly/2021-140-00-00. [Hozzáférés dátuma: 2025.11.04.].

[17] „2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról,” [Online]. Available: https://njt.hu/jogszabaly/2011-128-00-00.39#CI. [Hozzáférés dátuma: 2025.11.04.].

[18] „54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról,” [Online]. Available: https://njt.hu/jogszabaly/2014-54-20-0A. [Hozzáférés dátuma: 2025.11.04.].

[19] „Tűzvédelmi Műszaki Irányelvek,” [Online]. Available: https://www.katasztrofavedelem.hu/213/tuzvedelmi-muszaki-iranyelvek. [Hozzáférés dátuma: 2025.11.04.].

[20] „2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről,” [Online]. Available: https://njt.hu/jogszabaly/2024-84-00-00. [Hozzáférés dátuma: 2025.11.04.].

[21] Nemzeti Adatvédelmi és Információszabadság Hatóság, „A munkahelyen alkalmazott elektronikus megfigyelőrendszer alapvető követelményeiről (ajánlás),” [Online]. Available: https://naih.hu/files/Ajanlas-a-munkahelyi-kameras-megfigyelesr-l.pdf. [Hozzáférés dátuma: 2025.11.04.].

[22] „Az Európai Parlament és a Tanács (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezé,” [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/hun. [Hozzáférés dátuma: 2025.11.04.].

[23] „2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról,” [Online]. Available: https://njt.hu/jogszabaly/2011-112-00-00. [Hozzáférés dátuma: 2025.11.04.].

[24] A. Móré, „Nélkülözhetetlen biztonságtechnikai szabványok szakterületenként, tervezők, telepítők, karbantartók és üzemeltetők részére,” 2021. [Online]. Available: https://szakmaikamara.hu/files/images/Orszagos/Szabvanyok/Javasolt_szabvanyok_2102.pdf. [Hozzáférés dátuma: 2025.11.15.].

[25] „ISO 27001 Információbiztonsági Irányítási Rendszer (IBIR),” [Online]. Available: https://www.tuvsud.com/hu-hu/szolgaltatasok/audit-es-rendszertanusitas/iso-27001. [Hozzáférés dátuma: 2025.11.04.].

[26] „ISO/IEC 27001 - Információbiztonsági Irányítási Rendszer (IBIR) tanúsítása,” [Online]. Available: https://iws.hu/tanusitas/iso-iec-27001-informaciobiztonsag/. [Hozzáférés dátuma: 2025.11.05.].

[27] A. Saeckel, „Az ISO 27002 felülvizsgálata - Ezek a változások,” [Online]. Available: https://www.dqsglobal.com/hu/szolgaltatas/blog/az-iso-27002-feluelvizsgalata-ezek-a-valtozasok. [Hozzáférés dátuma: 2025.11.05.].

[28] Z. Reizinger, „Információbiztonsági szabvány változás,” [Online]. Available: https://quality-mmt.hu/2022/02/17/informaciobiztonsagi-szabvany-valtozas/. [Hozzáférés dátuma: 2025.11.05.].

[29] „AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2022. december 14-i (EU) 2022/2555 IRÁNYELVE 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,” [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a22i2555.eup. [Hozzáférés dátuma: 2025.11.05.].

[30] „Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (E,” [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555. [Hozzáférés dátuma: 2025.11.05.].

[31] „NIS 2 irányelv: hálózati és információs rendszerek biztosítása,” [Online]. Available: https://digital-strategy.ec.europa.eu/hu/policies/nis2-directive. [Hozzáférés dátuma: 2025.11.05.].

[32] Á. Kemendi, „Integrált kockázatkezelés,” *Biztonságtudományi Szemle,* pp. 43-61, 2022. IV. évf. 1. sz..

[33] Z. Zólyomi, Komplex biztonságmenedzsment, Budapest: Óbudai Egyetem Biztonságtudományi Doktori Iskola, 2019.

[34] G. Dr. Lukács, A. Dőring és P. Hell, Vagyonvédelmi Rendszerek I., Budapest: Óbudai Egytem Kandó Kálmán Villamosmérnöki Kar, 2015.

[35] G. Dr. László, Kockázatértékelés, kockázatmenedzsment, Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[36] Z. Reizinger, „Kockázatmenedzsment - új szabvány,” [Online]. Available: https://rendszerek.hu/kockazatmenedzsment-uj-szabvany-magyarul/. [Hozzáférés dátuma: 2025.10.08.].

[37] F. Gubics és T. Horváth, „A fizikai védelmi rendszerek és a biztonsági központ,” *Magyar Rendészet,* pp. 89-105, 2024/1.

[38] A. Pallagi és T. Kovács, „Kritikus infratruktúrák komplex biztonságvédelmi rendszereinek tervezése, kialakítása, különös tekintettel a beléptetőrendszerek alkalmazására,” *Hadmérnök,* pp. 35-45, 2019. 14. évf. 4. sz..

[39] „Data Center Group,” [Online]. Available: https://datacenter-group.com/en/products/dc-it-room/dc-it-room-granite/. [Hozzáférés dátuma: 2025.11.10.].

[40] „Samsung,” [Online]. Available: https://www.samsung.com/us/smart-home/security/security-systems/sdc-7440dc-varifocal-dome-camera-sdc-7440dc/. [Hozzáférés dátuma: 2025.11.15.].

[41] „Hörmann,” [Online]. Available: https://www.hormann.hu/ipar-kereskedelem-koezszfera/ajtok/funkcios-ajtok-intezmenyi-koernyezethez/. [Hozzáférés dátuma: 2025.11.10.].

[42] A. Braun és R. Pető, „Egy katonai radarobjektum élőerős védelmének megszervezése,” *Biztonságtudományi Szemle,* pp. 39-48, 2025. VII. évf. 3. sz..

[43] „1997. évi CLIX. törvény a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról," [Online]. Available: https://njt.hu/jogszabaly/1997-159-00-00. [Hozzáférés dátuma: 2025.10.25.].

[44] T. Berek és G. Bodrácska, „Az élőerős őrzés az objektumvédelem építőipari ágazatában," *Hadmérnök,* pp. 38-49, 2010. V. évfolyam 4. szám.

[45] A. Szabó, „A szabályzatok szerepe az objektumok őrzésvédelmében," *Műszaki Katonai Közlöny,* pp. 2-15, 2017. XXVII. évf. 1. sz..

[46] „Dormakaba," [Online]. Available: https://www.dormakaba.com/hu-hu/ajanlat/termekeink/belepteto-es-bejarati-rendszerek/forgokapuk/kerberos-haromkaru-forgovilla--ka_114687. [Hozzáférés dátuma: 2025.11.10.].

[47] „Specto-Net," [Online]. Available: https://spectonet.hu/eger/biztonsagi-kamerarendszerek-telepitese-kameras-tavfelugyelet-vagyonvedelem-biztonsagtechnika-terfigyelo-riaszto29/. [Hozzáférés dátuma: 2025.11.15.].

[48] „SecurInfo," [Online]. Available: https://www.securinfo.hu/termekek/kulteri-vedelem/8746-180-fokos-kulteri-mozgaserzekelo-szeria-az-optex-tol-wx-infinity-neven.html. [Hozzáférés dátuma: 2025.11.15.].

[49] Z. Zólyomi, „A biztonság és a biztonságmenedzsment vizsgálata vállalati nézőpontból," *Hadmérnök,* pp. 19-29, 2020. 15. évf. 1. sz..

[50] P. Michelberger, „Integrált vállalati kockázatmenedzsment - Lehetőségek és veszélyek a szabványok és ajánlások tükrében," *Biztonságtudományi Szemle,* pp. 25-34, 2025. VII. évf. 1. sz..

[51] „SecurInfo," [Online]. Available: https://www.securinfo.hu/termekek/kulteri-vedelem/14729-keruletvedelmi-piaci-tendenciak-proaktivitas-es-tobbreteg-vedelem.html. [Hozzáférés dátuma: 2025.11.30.].

ÁBRAJEGYZÉK