ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

BRÉDA GÁBOR

Védett helyiségek komplex biztonsága

Témavezető: Dr. Varga Péter János PhD

**BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA**

Budapest, 2022. október 25.

Szigorlati/komplex vizsga bizottság:

Elnök:

Prof. Em. Dr. Berek Lajos professor emeritus

Tagok:

Dr. habil. Farkas Tibor egyetemi docens, külső - NKE

Dr. habil. Berek Tamás egyetemi docens, külső - NKE

Nyilvános védés teljes bizottsága:

Elnök:

Prof. Dr. Rajnai Zoltán egyetemi tanár, ÓE

Titkár:

Dr. Pető Richárd adjunktus, ÓE

Tagok:

Dr. habil. Farkas Tibor egyetemi docens, külső - NKE

Dr. Szűcs Endre, külső

Prof. Em. Dr. Berek Lajos professor emeritus

Bírálók:

Dr. habil. Dobák Imre egyetemi docens, külső - NKE

Dr. Schuster György egyetemi docens, ÓE

Nyilvános védés időpontja:

NYILATKOZAT A MUNKA ÖNÁLLÓSÁGÁRÓL, IRODALMI FORRÁSOK MEGFELELŐ MÓDON TÖRTÉNT IDÉZÉSÉRŐL

Alulírott **Bréda Gábor** kijelentem, hogy a **Védett helyiségek komplex biztonsága** című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem egyértelműen, a forrás megadásával megjelöltem. Az értekezés elkészítéséhez, nyílt forrásból származó anyagokat használtam fel.

Budapest, 2022. október 25.

Bréda Gábor

TARTALOMJEGYZÉK

BEVEZETÉS

Az információ a modern civilizációnk egyik legfontosabb alkotóeleme és hajtómotorja. Birtoklásának és megtartásának egyre nagyobb a jelentősége. Korunk fejlődő világában a technológiai fejlettség elérte azt a szintet, hogy a környezetünkben megjelenő, az ember számára közvetlenül érzékelhető és érthető vizuális információk, valamint akusztikus hangok technikai megoldásokkal detektálhatók, észrevétlenül rögzíthetők és továbbíthatóak a világ bármely pontjára. Az adatokból kinyert információ szenzitivitása szférától és szektortól függetlenül nagy fontossággal bírhat, jelentős értéket képviselve az adatbirtokosok számára. Ezért kiemelt fontosságú lehet azok védelme, indokot teremtve védelmi intézkedések kialakítására. A kutatásom a kommunikáció műszaki - információbiztonsági vonulatának erősítésére fókuszál. Olyan környezet megalkotására, ahol a közvetlen ember - ember közötti kommunikációs interaktus során elhangzó és vizuálisan megjelenő információtartalom csak a résztvevők számára nyilvános, ott harmadik fél jelenléte, valamint információ megszerzésére alkalmas technológia jelenléte szavatolt formában kizárt. A munka során meghatározom a téma szempontjából releváns „védett helyiség” fogalmát, mely tisztázza a kutatás címének egyértelmű azonosítását. A vizsgálat kiterjed a fellelhető magyar jogi források elemzésére, melyek tanulmányozása során kutatom, hogy a témában specializált, az elhangzott szó és a vizuálisan megjelenő szenzitív tartalom védelmére irányuló definiált intézkedések meghatározására született-e előírás. Áttekintem az információelmélet alapjait és tisztázom az adat és információ fogalmi eltéréseit. A munka során a további kutatásaimat műszaki irányban folytatom, mivel a disszertációm célja egy elvi modell felállítása a védett helyiség kialakítására. A feltárás során áttekintem a téma szempontjából meghatározó, az információbiztonsági problémát jelentő hírszerzési módokat majd áttekintettem a kommunikációs folyamatokhoz szorosan kapcsolódó fizikai jelenségeket. Ezt követően feldolgozom a témában nyílt forrásból elérhető, közvetlen az információbiztonságot fenyegető lehetséges technikai megfigyelő eszközök fizikai jellemzőit, különös tekintettel az alkalmazhatóságukhoz szükséges műszaki feltételekre, és az átviteli utak jellegére. A megismert paraméterek függvényében javaslatot teszek egy lehetséges védett helyiség elhelyezésére, majd egy elvi modellen keresztül bemutatom annak egy lehetséges kialakítását. A védett helyiség modelljének kialakítása során figyelembe veszem a kutatás során megismert technikai eszközök paramétereit, így a kutatásom egyik

eredményeként javaslatot teszek olyan kialakításra, amely kizárja a nem kívánt technológia jelenlétét, vagy megakadályozza azok működését. Áttekintem a témában releváns akusztikus és rádiós csillapításra vonatkozó, nyíltan hozzáférhető forrásokat, és javaslatot teszek csillapítási értékeinek alkalmazására. A lokalizáció elősegítése érdekében, a védett helyiségek üzemvitele során felmerült a rádiós sugárforrások lokális azonosításának szükségessége, melyre egy új típusú rádió-vevő berendezés használatát javaslom. A téma feldolgozása során felmerült a védett helyiségekben kialakítani kívánt vezetékes kommunikációs csatorna létrehozásának igénye, melyre az optikai távközlési megoldás kialakítása bizonyult a legmegfelelőbbnek, amelyet átfogó szálellenőrzési rendszer beépítésével javaslom kialakítani (V. fejezet; 2. számú melléklet). A disszertáció részeként javaslatot teszek védett helyiségek fenntartására és üzemeltetésére a folyamatos információbiztonsági egyenszilárdság fenntartásának biztosítása érdekében. A jogalkotó számára javaslatot teszek a meglévő jogi szabályzók műszaki tartalmának kiegészítésére. Javaslatom a minősített adat szóbeli megjelenési környezetének biztonságosabbá tételére irányul, a szóbeli kommunikációs interaktus helyszínének ajánlott technikai átvizsgálási műveleteinek meghatározásával.

A téma aktualitását bizonyítja a szabadon beszerezhető, technikai úton működő, autonóm információszerző eszközök elérhetőségének nagymértékű növekedése, a kommunikációs technológiák gyors fejlődése, valamint a médiában egyre sűrűbben hallott, a témához kapcsolódó közlemények megjelenése.

A kutatás egyes fejezetei az elektronikus hírszerzés önálló hardverelemeinek műszaki feldolgozását, valamint a működésük megakadályozására létrehozott környezet kialakítását tárgyalja. A kutatás során fellelt eszközök és módszerek, nem lehetnek reklám és alkalmazástechnikai ajánlás tárgyai. Ezért az erről szóló fejezetek szűken tárgyilagosak, a téma tárgyalásához nélkülözhetetlen konklúziókat és bárki által elérhető információt tartalmaznak.

A kutatásomhoz és disszertációmhoz, nyílt forrásból származó információkat használtam fel.

A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

A kutatásom az információbiztonság megteremtésének sajátságos technikai területével foglalkozik, amely az ember - ember közötti közvetlen kommunikáció környezetének információbiztonsági védelmét célozza. Az elérhető előírásokban a téma alapját adó előzetes kutatást végeztem. A tanulmányozás során célzottan olyan előírásokat kerestem a kommunikációs környezet védelme érdekében, amelyek konkrét műszaki tartalmat határoznak meg. Kutatásom alapján az adat tárolására, az adathordozókon illetve informatikai rendszerben tárolt adatok védelmére, - különösen, ha azok szenzitívek, vagy minősítéssel rendelkeznek - elérhetőek fizikai védelmet célzó előírások. Minősítés esetén a törvény által deklarált rendelkezéssekkel védik az adatokat, mind személyi feltétel, mind az adathordozó fizikai védelmének oldaláról. A témában elérhető előírások alapján bebizonyosodott, hogy a különböző titokvédelmi és jogi eszközöket is figyelembe véve a szenzitív vagy minősített adatokat - információt - tartalmazó elhangzott szó és a vizuálisan megjelenő szenzitív tartalom fizikai környezetének konkrét kialakítására nem található egyértelműen meghatározott ajánlás.

Az információ emberek közötti feldolgozása és megosztása a beszéd, látás és hallás útján lehetséges, amely megfigyelhető. Az előírásokkal és szabályokkal, műszakilag védett környezetből kikerülő információ olyan közegbe kerülhet, amely biztonsági szintje nem egyezik a tároló rendszer biztonsági szilárdságával. Az információ megjelenése új formát ölt, a kommunikáció során a tároló rendszertől eltérő új fizikai jellemzőkké alakul, amely technikai berendezésekkel megfigyelhető.

A kutatási témám az ember- ember közötti közvetlen kommunikáció során előálló hang és vizuálisan megjelenő információ fizikai védelmére irányul. A szakirodalmi kutatás során találtam olyan hazai és külföldi ajánlásokat, leírásokat, amelyek részben kapcsolódnak a problémakörhöz, de egyértelmű ajánlást vagy hozzáférhető, megfelelő intézkedési utasítást nem adnak. Kutatásom célja, egy olyan környezet megteremtése, ahol az információ nagyfokú biztonságának egyenszilárdsága garantálható az elvi biztonsági rések kiküszöbölésével. Feltételezem, hogy létrehozható egy védett környezet modell szintű megalkotása, amely mint védett helyiség definiálható.

AZ ÉRTEKEZÉS TÁRGYA ÉS CÉLKITŰZÉSEI

Az értekezés tárgya

Egy olyan fizikai környezet, és a környezethez kapcsolódó paraméter rendszer felállítása, ahol az ember-ember közötti kommunikáció analóg módon, úgy valósulhat meg, hogy a kommunikáció során akusztikusan elhangzó információ, vagy vizuálisan megjelenő információs tartalom, csak a kommunikációs környezeti térrészben jelenlévő személyek számára válhasson megismerhetővé. A kommunikációs környezet elemei ellenőrzött és szavatolt módon, homogenitással rendelkeznek, kizárva minden olyan, technikai információszivárgási csatorna és lehetőség jelenlétét, amely a kommunikáció során megjelenő elsődleges és másodlagos fizikai jellemzők érzékeléséből elvi lehetőséget nyújtanak az információ harmadik fél számára való közvetlen vagy közvetett megismerésére. A kutatás eljárások és fizikai kialakítások összességét helyezi új kontextusba. Az elsődleges feladat a meghatározott biztonságos környezet kialakításának elvi megvalósítása, a felmerülő elméleti biztonsági rések kiküszöbölése révén.

Az értekezés célkitűzései

- Meghatározni a "védett helyiség" fogalmát;
- Megvizsgálni a jogi forrásokat, igazolva a téma relevanciáját, igazolva az előzetes kutatások állítását;
- Javaslatot tenni egy megfelelő védett tárgyaló helyiség épületen belüli elhelyezésére,
- Igazolni az analóg módon előálló információcsere során létrejött információszivárgási csatornák kialakulását;
    - Igazolni demonstrációval az akusztikus hangrezgések terjedését a védeni kívánt kommunikáció során használt helyiségek határoló falazatában és azok szomszédos környezetében az információszivárgási lehetőségek igazolására;
    - Igazolni az optikai úton történő információszivárgás tényét;
    - Igazolni a megjelenítő eszközök nem üzemszerű rádiófrekvenciás sugárzásait a kisugárzott információtartalom tekintetében;
    - Igazolni a rádiós árnyékolás, mint védelmi intézkedés szükségességét;

- Áttekinteni a technikai információszerzés lehetséges autonóm módjait, majd rendszerezni a nyílt forrásból megismerhető fenyegetést jelenő technikai eszközök fő működési paramétereit;

- Meghatározni a védett helyiség kialakításának elvi modelljét
  - Javaslatot tenni védett helyiség tekintetében akusztikai és rádiós árnyékolás csillapítási értékeire;
  - Javaslatot tenni védett helyiségek közötti pont - pont összeköttetés megvalósítására a fizikai réteg monitorozhatóságának tekintetében;
  - Javaslatot tenni felhasználható prezentáló eszközök optimális szoftver technológiai paramétereinek meghatározására;
  - Javaslatot tenni védett helyiségek kialakítása és üzemeltetése során szükséges vizsgálatok kialakítására;
  - Javaslatot tenni és elvi megoldást adni a védett helyiségek környezetében megjelenő rádiós források lokális közeltéri azonosítására, az épített környezet rádiós csillapítási jellemzőinek figyelembevételével;
- Áttekintést adni kiegészítő rendelkezés megalkotásához a minősített adat szóbeli megjelenési környezetének biztonságosabbá tételéhez, a szóbeli kommunikációs interaktus helyszínének ajánlott defenzív átvizsgálási műveleteinek meghatározásával.

A téma jelenőségét tekintve specifikus az információbiztonság - fizikai rétegének - kialakítása területén, mivel a hagyományos mechanikai - fizikai, elektronikus vagyonvédelmi és objektumvédelmi elemek ugyan részei a kutatás tárgyát képező helyiség biztonsági elemeinek, azonban azok az elvi feltételezések révén, nem képesek teljes mértékig biztosítani a téma szempontjából megfelelő biztonság kialakítását. A kutatás kimenete a feltárt kockázatok ismeretében speciális, az objektumvédelemben nem megszokott, technikai-információvédelmi műszaki intézkedések alkalmazásának feltárása, az elvi információbiztonsági rések kiküszöbölése, a védett helyiség modelljének kialakításának céljából.

A TÉMA KUTATÁSÁNAK HIPOTÉZISEI

Témaválasztás

Napjaink információbiztonsági horizontjához kapcsolódik az ember-ember közötti kommunikáció biztonságos környezetben történő megvalósítása, amely különleges tématerületet jelent a biztonságtudomány területén. Az értékkel bíró információk védelme során, szélsőséges felületnek számít az információmegosztás helyszíne és módja. A biztonsági szempontból tudatos kommunikációnak szerves részét kell, hogy képezze a megosztás helyszíne, így a védett helyiség használata a kommunikáló felek számára. A téma kutatási irányait tekintve, a témához kapcsolódó tudományterületek széles skáláját elemzés alá vontam. A téma teljes feldolgozására többnyire a műszaki irányt választottam, azonban interdiszciplináris összefüggéseket is igyekeztem keresni. A kutatás térképét az 1. számú mellékletben ábrázoltam. A témában a következő hipotéziseket fogalmaztam meg:

Hipotézisek

H1. számú hipotézis: Feltételezésem szerint megfogalmazható a védett helyiségre egy általános megfogalmazás, amely mindenki számára érthetővé és konkréttá teszi a témában megfogalmazott védett helyiség fogalmát.

H2. számú hipotézis: Feltételezésem szerint rendszerezhetők az állami és magán szektorok intézményrendszerei, melyekben ajánlott a védett helyiségek kialakítása.

H3. számú hipotézis: Feltételezem, hogy megalkotható olyan védett helyiség struktúra, amely a besorolt állami és magánszektorban megvalósítható.

H4. számú hipotézis: Feltételezésem szerint csoportosíthatók az egyedi eszközös elektronikus információszerzés elemei és kommunikációs útjai melyek fenyegetést jelentenek a védett helyiségben megjelenő információra. Valamint a működési paraméterek tekintetében adható olyan műszaki megoldás, amely defenzív hatással van a folyamatra.

H5. számú hipotézis: Feltételezésem szerint demonstrálható az ember- ember közötti közvetlen kommunikáció során kialakuló, fizikai jelenségek okozta információbiztonsági kockázat.

H6. számú hipotézis: Feltételezésem szerint megalkotható egy olyan komplex védelmi megoldás rendszer, mellyel megvalósítható és biztonságosan üzemeltethető egy védett helyiség.

H7. számú hipotézis: Feltételezésem szerint, meghatározható olyan adatátviteli csatorna kialakítására alkalmas módszer, amely védett helyiségek pont - pont adatkapcsolati összeköttetésének igénye esetén, ellenőrizhető megoldást nyújt a fizikai réteg épségének ellenőrizhetősége szempontjából.

KUTATÁSI MÓDSZEREK

1. Irodalomkutatást és elemzést végeztem a témához kapcsolódó hazai jogi dokumentumok vonatkozásában;
2. Irodalomkutatást és elemzést végeztem a témához közvetlenül kapcsolódó források tekintetében;
3. Irodalomkutatást és elemzést végeztem az adat és információ elméleti definiálásának pontos meghatározása érdekében, a témához kapcsolódó tudásmenedzsment diszciplína tudományág területén;
4. Kutatást és elemzést végeztem, nyílt forrásból elérhető, a témában meghatározó hírszerzési módszerek tekintetében, az információbiztonságot befolyásoló problémacsoport behatárolása érdekében;
5. Kutatást és műszaki elemzést végeztem a védelmi intézkedések pontos meghatározása céljából, a nyílt forrásból elérhető, a védett helyiség technikai információbiztonságát növelő technológiák tekintetében;
6. Gyakorlati kutatást folytattam az ember-ember közötti közvetlen kommunikáció során megjelenő fizikai jelenségek terén, a felmerülő probléma sajátosságainak feltérképezése érdekében;

7. Megvizsgáltam és összegeztem a feltárt elvi információbiztonságot veszélyeztető komponenseket, következtetéseket vontam le belőle, majd ezen következtetések alapján javaslatot tettem a lehetséges védelmi alkalmazási eljárásokra;
8. Kísérleteket, méréseket hajtottam végre a célokban megfogalmazott akusztikai és rádiótechnikai fizikai jellemzők igazolásához, melyek eredményeiből következtetéseket vontam le;
9. Kutatási eredményeimet tudományos konferenciákon ismertettem mind itthon, mind külföldön magyar, illetve angol nyelven;
10. Eredményeimet a konferenciákon túlmenően, lektorált folyóiratokban is publikáltam;

A kutatás lezárásra került 2021. május 15-én.

Alaki és formai megjelenés

A szakirodalomi hivatkozásokat az értekezés törzsszövegében az előfordulás sorrendjében, a műszaki szakirodalmi hivatkozásoknak megfelelően szögletes zárójelben" [ ] ", számmal ellátva alkalmaztam és az „Irodalomjegyzék” fejezetcím alatt rendszereztem. A megjegyzéseimet a sorszámozott lábjegyzetben fejtettem ki. A disszertációban megjelenített ábrákat az " Ábra jegyzék " című fejezetben sorolom fel. A disszertációban megjelenített táblázatokat a " Táblázat jegyzék "fejezetben sorolom fel. A mellékletek részben a folyószövegben hivatkozott melléklet elnevezésű ábrák kerültek elhelyezésre.

I. AZ INFORMÁCIÓ ÉS A VÉDETT HELYISÉG

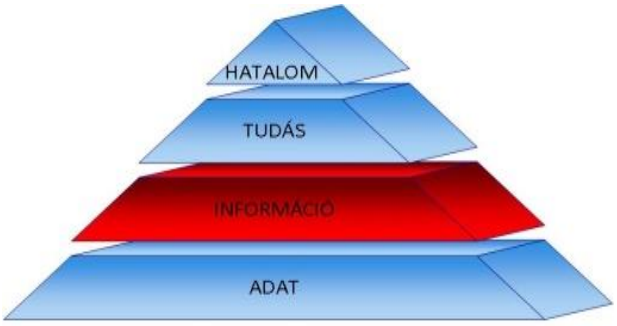
Jelen fejezet célja az első hipotézispontom igazolása. Az adatfeldolgozásból nyerhető információ, értékkel rendelkező eredményt teremt. Az értékes információ megosztásának elsődleges módja a személyes kommunikáció. A kommunikáció helyszínét illetően olyan biztonsági kérdések merülnek fel, amelyekre egy védett környezet jelenthet megoldást.

BEVEZETÉS

Napjainkban az adatok fizikai és adminisztratív védelme jól szervezettnek tekinthető. A keletkező adatok tárolása szinte kizárólag informatikai rendszereken valósul meg. Az adatokból készített információk védelmének áttekintése során, egy feltételezhető információbiztonsági rés tapasztalható, amely az internet elterjedésével, valamint a technológiák fejlődésével aktuális problémát okoz az információvédelem egyenszilárdságának kialakításában. Korunk információs társadalmában a nap 24 órájában folyamatosan keletkeznek adatok, amelyek lehetnek nyíltak vagy korlátozott hozzáférésűek. Az adatokat a megfelelő minőség és kapacitás elérése érdekében, rendszerint adathordozón vagy informatikai rendszeren tárolják. Az adatfeldolgozás és az eredmény tárolása is mára szinte kizárólag informatikai eszközökön történik, amely a nem a nyilvános adatok védelme érdekében jelentősen felértékeli a védelmi kialakítások létrehozásának fontosságát. Az adatok védelmével törvényi szinten a jogalkotó, míg az informatikai eszközök és hálózatok védelmével, mint az információs társadalom alapvető információ-megosztói környezetével világszerte számos szervezet foglalkozik. Az adathordozókra rögzített adatok és információk védelmére alkotott mechanizmusok túlnyomórészt egy helyiség vagy épületkomplexum meghatározott falai közé szorulnak. A napi valóság élethelyzeteit áttekintve azonban megállapíthatjuk, hogy azok nem csak rögzített formában és az erre kialakított zárt és szabályozott rendszerben fordulnak elő, hanem más környezetben is, sokszor a szokások által befolyásolva. Jelen fejezet sorain keresztül az adat és információ összefüggését vizsgálom, majd definiálom a fennálló biztonsági rést és a téma szempontjából meghatározott védett helyiség fogalmát.

1.1. Adat és információ

A hétköznapi kommunikációban sokszor beszélünk adatról, információról, a fogalmakat egymás szinonimájaként használva. Az adatokat birtokolni és ismerni, nem jelenti önmagában azt, hogy információ birtokában vagyunk. Ha információink vannak, az sem jelenti azt, hogy tudásunk lenne. Életünk minden területén az tapasztalható, hogy jelentős mennyiségű adat keletkezik és halmozódik fel. Ez minden bizonnyal idővel majd egy túlcsordulást okoz, amely újabb problémákat fog a felszínre hozni. A világban történő bármilyen változás mára már szinte minden esetben valamilyen adatot generál. A megfelelő mennyiségű és minőségű adat azonban a döntések alapjául szolgál. A tárolt adatok mennyisége ellenére viszont nem egyértelmű mindig, hogy mi a kimeneti cél. Nincs minden esetben kimeneti koncepció. Az emberré válás korai szakaszán rájöttünk, hogy az információ birtoklása előnyhöz segít a kevésbé tájékozott féllel szemben. Az emberiség történelmében, eddig még soha nem látott minőségű és gyorsaságú hírközlési berendezések állnak a hétköznapi ember rendelkezésére. Tulajdonképpen a nagy kihívást manapság, nem az adatok megszerzése és tárolása, hanem az azokból nyerhető információ létrehozása, valamint hasznosítható formába történő alakítása jelenti. A köznapi nyelvezetben a következő szavakat egymás szinonimájaként használjuk, pedig mégis nagy különbség van közöttük. Az adat és az információ jelentése eltérő. Russel L. Ackoff által megfogalmazott elméleti kapcsolatot egy piramis modellben vizsgálhatjuk szemléletesen az 1. számú ábrán. [1]



1. ábra Az adat - információ - tudás - hatalom kapcsolati modellje (Forrás [1] alapján saját szerkesztés)

Az adat az alappillér, melynek feldolgozásával juthatunk az információhoz. Az információk összessége olyan tudást képezhet, amely hozzájárulhat a bölcsesség, vagy hatalom kialakulásához. A tudás és a hatalom elemek a tulajdonképpeni információszerzésből kapható célfüggvények, melyek az egyéni javak gyarapodását

gyökeresen befolyásolják. Az adatok gyűjthetőek automatikus rendszerek útján, de a további feldolgozásuk során képesnek kell lenni megfelelő jelentéssel felruházni azokat. Az adatok gyűjtése során szem előtt kell tartani az abból előállítható információt, illetve a megszerezni kívánt tudást. Míg az információ sajátos jelentésjelleggel bír, addig a tudás az információk birtoklójának újabb lehetőségeket kínál. Egy információ, az alapjául szolgáló adatok révén, több beágyazott jelentéstartalmat is kifejezhet. [2]

A megfelelő tudáshalmazok logikai kezelésével bölcsesség és hatalom érhető el, amely logikai rendezéssel további döntéstámogató értéket képvisel. Az információkból rendelkezésre álló tudás, elengedhetetlen a jó döntések meghozatalához. [3] [4] [5]

A tudásszintet tovább elemezve, Polányi M. megállapításai szerint a tudást kétféle módon értelmezhetjük. [2] Egyik módja a rejtett, a másik a közvetlen tudás. Míg a rejtett tudás a tapasztalatokon, emberi tulajdonságokon, szándékon, képzeleten, kreativitáson és helyzetfelismerésen alapul, úgy a közvetlen tudás direkt módon kapcsolódik az információhoz a racionális logikus gondolkodáshoz. Fontos megállapítás továbbá, hogy a tudás nem alakul ki magától. A tudás egy folyamat terméke, azaz keletkezik. Nonaka és Takeuchi kutatásukban használták Polányi tudáskategóriáit, elméletük szerint tudást lehet szerezni az információk ismeretéből, megérteni az üzenetét a már létrehozott tudásnak. [2] [6] Továbbá létezik az a fajta tudás, amely az adatok saját feldolgozásából ered, így az információ, majd a tudás a megalkotójuk munkáján keresztül válik kész értékké. Érdekes megállapítás, hogy a rejtett, vagy úgynevezett hallgatólagos tudás mechanikáját nehéz megértenünk, mert mint a már említett módon nagyban emberi tényezőktől függ. A közvetlen tudás mechanizmusa viszont jól áttekinthető, hisz ez a fajta információ alapú tudás, világos belső logikájú és könnyen átadható. A közvetlen tudás mechanizmusa első lépésként elmagyarázza a mögöttes logikát, majd biztosítja a hiányzó adatokat és információkat. Amennyiben a meglévő adatokat logikai úton különböző formában kombináljuk új adatokkal, úgy új információk előállítása válik lehetségessé.

A jó döntések meghozatalához lényeges az adatok megfelelő elemzése, a helyes összeillesztés és az információ előállítása. Egy probléma megoldása során, minél több információ áll rendelkezésünkre, annál megfelelőbben lehet meghatározni a lehetőségeinket. Azonban a teljes tudás megszerzése az összes információ magunkévá tétele szinte lehetetlen feladat. Előfordul, hogy nincs elég időnk, vagy nincs hozzáférésünk, vagy elég anyagi erőnk megszerezni mindet. Amennyiben egy döntés

előtt meg tudnánk szerezni minden információt, akkor lehetséges, hogy annak mennyisége olyan hatalmas mértéket öltene, hogy nem tudnánk azt feldolgozni. A döntések velejárója nagy általánosságban az információ hiánya és a bizonytalanság, így válik értékké a megszerzett információ mennyisége és pontossága. Az információt, mint döntéssegítő tudást értékelve, a jó információ lehet: pontos, időszerű, átfogó, alapos. [7] [1]

Összegezve, egy információ nem mondja meg, hogy mit kell tennünk, csak segíti a feladat végrehajtását. Az élet adta döntési helyzetek nem sablonosak, minden esemény saját körülményei környezetében zajlik, így nem tudunk pontos modellt adni egyik helyzet megoldására sem. Amennyiben az információ korlátlan mennyiségben hozzáférhetővé válik az ember számára, akkor a következő akadályt maga az ember jelenti, mert korlátozott az információ feldolgozó kapacitása, ezáltal saját magát hátráltatja. [8] [9] [10]

A tárgyaltak miatt válik fontossá, hogy adott témát illetően, értékkel bíró kész információkhoz juthassunk, amelyek a döntési bizonytalanságot megfelelően kompenzálhatják [11]. A fentiek alapján az okfejtésből kiindulva, az információ jelentős értékké válása miatt válik nélkülözhetetlenné az információ védelmének teljes körű kialakítása. A védelem kialakítása kapcsán fontos elvi felvetés, hogy a védelmi költségeknek arányban kell állnia a védeni kívánt információ értékével, mivel az információ értékét túlhaladó védelmi beruházás költsége gazdaságtalanná teszi a beruházás megvalósítását. [12]

1.2 Információbiztonság, megjelenő információbiztonsági rés

A biztonság, egy összetett fogalom. A téma szempontjából a teljes spektrumot vizsgálva ki kellett választanom azt a részt, amely terjedelmét tekintve belefér a kutatás kereteibe. Az információbiztonság az információ sértetlenségének, bizalmasságának és rendelkezésre állásának megőrzését célzó intézkedés. [13] A jelen kutatás szempontjából a bizalmasság fogalmi körébe tartozó fenyegetettség kizárása a cél. A téma vizsgálata során az adat, mint az információ legkisebb egysége általában valamilyen adathordozón, rögzített formában áll rendelkezésre. Amennyiben hagyományos papír alapú, vagy digitális adathordozóról van szó, kézzel fogható meghatározható méretű tárgyról beszélünk, amelyet a méreteitől függően a biztonságtechnika és a kriptográfia módszereivel, bevált szisztémák alkalmazásával az

illetéktelen hozzáférés elől jól védhetőnek tekintek. A fent leírtak alapján az adatok nyersen, önmagukban nem feltétlenül fejeznek ki értelmezhető hasznos információt. Ahhoz, hogy információvá váljanak, fel kell dolgozni azokat. [1] [3] [6] Az adatfeldolgozás napjainkban szinte kizárólag a számítástechnika eszközeivel történik, és a feldolgozást követően az információ digitális formában, informatikai eszközön rögzül. Az informatikai információbiztonság szintjét jelen kutatás során a biztonsági rés megjelölésének szintjén kezelem, az informatikai IT biztonság kialakítása nem jelen kutatás tárgya. A digitális információ tartalmakat, az adat és információbirtokosok szemszögéből megfelelően biztonságosnak tekintem.

A téma tekintetében a tudáshoz vezető utat megvizsgálva láthatjuk, hogy a tudás egy emberi jellemző, az csak személyhez kötött formában érhető el. Az embernek, mint létező, élő materiális információhordozónak a védelmére a személyi védelem megszervezése lehet a megfelelő védelmi intézkedés, amelyet a kutatás szempontjából megfelelő szintűnek tekintek.

Továbbá az egyén szempontjából az információbiztonság fenntartása céljából az egyéni biztonságtudatos viselkedése a meghatározó. A humán információszerzés, a social engineering, a téma további nagysága miatt szintén nem jelen kutatás iránya, azonban a témából kiindulva egy további kutatás alapját teremtheti meg. [14] [15] [16] [17] [18]

Jelen kutatás fő irányát az ember-ember közötti közvetlen kommunikációs interakció során megjelenő fizikai jelenségek és a megjelenítő interfészek alkalmazása során megjelenő információszivárgási csatornák kutatása képezi. A tudás humán megosztása során létrejövő, a bizalmasságot veszélyeztető kockázatok csökkentése a kommunikációs tér biztonságossá tételével, védelmi megoldások bevezetésével alakítható ki.

Napjainkban az információ megszerzése és továbbítása a rendelkezésre álló technológiai háttér miatt nem jelent már akkora akadályt, mint pár évtizeddel ezelőtt. Mivel az adat és az információ digitális rögzítése, valamint áramoltatása az infokommunikációs rendszerekben a technológiák tervezett alapfunkciója. Nehéz gátat szabni az információk rendszerbe történő szelektív bekerülésének és így azok terjedésének.

Századunk felgyorsult világában, az információhoz való gyors hozzáférés, valamint a hírközlő technológiák alkalmazása napi szintű gyakorlattá vált. Míg a 90-es években pár száz MB információ elektronikus úton történő rögzítésére, valamint annak továbbítására való eszköz, átlagember számára szinte hozzáférhetetlen és megfizethetetlen technológia volt, [19] [20] addigra napjainkban szinte bárki hozzáférhet nagy tudású

elektronikus kommunikációs készülékhez, akár anonim módon internetes vásárlás segítségével is. A kutatás előzményeként feltárásra került, hogy az elektronikus - kommunikációs és audiovizuális rögzítő eszközöknek kialakult egy speciális iránya, amely a kisméretű - rejthető eszközök piacát célozta meg. A világhálón található kínálatot megvizsgálva szembetűnik, hogy egy egész iparág épült kisméretű információgyűjtő - rögzítő berendezés fejlesztésére és gyártására melyet a IV. fejezetben ismertetek.

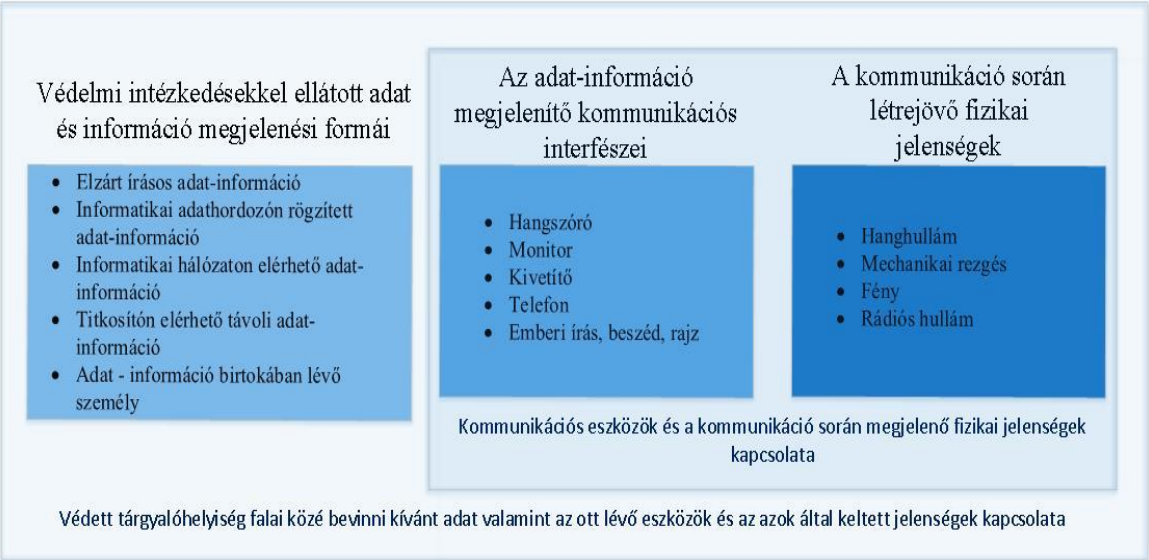
Az ilyen eszközökkel történő információszerzés, normál esetben csak különböző jogi normáknak megfelelve, törvényi felhatalmazás által történhet. Azonban a valóságot megvizsgálva, és a napi sajtót szemügyre véve gyakran találunk olyan közleményt, amelynek tartalma etikátlan technikai hírszerzési metódusból származhat, illetve maga az etikátlan elektronikus információszerzési módszer ténye, eszköze kerül napvilágra. Hazánkban a jogosult szervezetek, külön engedély birtokában alkalmazhatják az ilyen módszereket és technikákat. Az elektronikus technikai hírszerző berendezések, gazdasági haszonszerzés vagy aljas indokból történő használata tilos, a Büntető Törvénykönyvről szóló 2012. évi C. törvényben (Btk.) szankcionált. [21] [11] [14] Mégis újból és újból kiderül, hogy létezik engedély nélküli információszerzés. A tiltott módon történő információszerzés alapvető technikai eszköze az elektronikus lehallgató berendezés. A probléma forrása az ilyen eszközök civil társadalmi közegben való jelenléte. A szóban forgó eszközök illetéktelen helyen való alkalmazása, az ember fizikai környezetének érzékelésével, elektronikus úton tárolva vagy továbbítva lehetőséget teremtenek harmadik fél általi információ megismerésére. Ezzel esetleges károkat okozva az információ jogos birtokosának, megsértve az adott információ bizalmasságát.

Az okfejtésből kiindulva merül fel az igény olyan személyes kommunikációs környezet megvalósítására, ahol a humán kommunikáció (megbeszélés - tárgyalás) biztosítható módon, kizárólag a jelenlévő felek közt hangzik el, és az elhangzott információ a kommunikációs környezeten belül marad, harmadik fél vagy információszerző technológia teljes kizárásával. A téma szempontjából az ilyen „bizalmi”- szenzitív kommunikációra alkalmas környezet megvalósítása a cél. A kutatás szkópját szűkítve, eljutunk a kutatási téma forrásához. Ahhoz, hogy az ember számára értelmezhető legyen egy adathordozón rögzített információ, és annak logikai kapcsolatából tudást szerezhessen, valamilyen kommunikációra van szüksége, vagyis meg kell, hogy ismerje azt. A megismerésnek fő érzékszerveink adhatnak lehetőséget, a hallás és a látás. [22]

Az adathordozón lévő információnak az ember számára értelmezhető formában történő megjelenítése a megjelenés kezdeti pillanatától a végéig az átviteli láncban olyan újabb elemeket hoz létre, amelyeknek az illetéktelenek elleni védelme a megoldandó feladat. A rögzített információk megismeréséhez interfészek kellenek, az átvitelhez alkalmas minőségben. Ezek az interfészek hang alapú átvitel esetén az emberi kommunikáció hangja, vagy a médiatartalmat lejátszó berendezés hangszórója által keltett hang rezgése. Vizuális átvitel esetén, az írásjelekkel ellátott papír, vagy a különböző monitorok, kivetítők információ tartalmú fénye. A láncban megjelenik több olyan fizikai jelenség, amelyeknek a hatását információbiztonsági szempontból meg kell vizsgálni és elvi információbiztonsági rés fennállása esetén a lehetséges csatorna elzárása érdekében védelmi megoldásokat kell kialakítani.

A védelmi egyenszilárdság elvét szem előtt tartva, ha egy, az adathordozók és informatikai rendszerek magas szintű védelmével felszerelt környezetben mindent megteszünk az információbiztonság megvalósítása érdekében, akkor az objektumvédelem a fizikai védelem és az informatikai elemek védelme mellett, nem hagyható figyelmen kívül annak a speciális környezetnek az információbiztonságilag megfelelő kialakítása sem, ahol azok kikerülnek a védett rendszerből és tisztán emberközeli formában jelennek meg.

A védeni kívánt fizikai jelenségeket szétválaszthatjuk direkt és indirekt módon megjelenőnek. Direkt módon a hang a levegő által szétterjed egy helyiség falai közt és a beszéd erősségétől függően megrezgeti a bent lévők dobhártyáját és az összes közeli tárgy felületét. A vizuális megismerés esetén a fény fotonjai az írott adathordozóról visszaverődés útján, monitor, kivetítő esetén fény kibocsájtás útján kerülnek a helyiség falai közé, majd a levegőn áthaladva a résztvevők szemébe, valamint a megjelenítő eszköz teljes betekintési szögének terébe. Indirekt módon előálló jelenségek az alkalmazott berendezések működéséből fakadó információ tartalmú elektromágneses kisugárzások, a hang által megrezgetett tárgyakban terjedő további rezgések, valamint a fény terjedése és tükröződése során létrejövő szórt nyalábok. [23] [24] Miután az ember érzékszerveihez eljutnak az említett információt hordozó fizikai jelenségek, és ha hallják és értik az adott nyelvet, valamint látják és értelmezik az írásjeleket és ábrákat, részesei-tudói lesznek az eddig szigorú műszaki követelményekkel és megoldásokkal védett adathordozókon lévő információknak. A megjelenő probléma elemeit összegezve a 2. számú ábrán láthatjuk.



2. ábra A kommunikáció védett és megjelenő elemei Forrás: saját szerkesztés

Az információ bizalmasságát sértő probléma ott jelentkezik, hogy az emberi találékonyság és az előzőekben említett műszaki kereskedelem adta kínálat segítségével lehetőség adódott olyan érzékelő, rögzítő célberendezések elterjedésére, amelyekkel autonóm módon megfelelő minőségben lehet akusztikus rezgést, valamint vizuális eseményeket érzékelni, rögzíteni, továbbítani. Konkretizálva, a legegyszerűbb példát véve, a legtöbb mobil-telekommunikációs készülék az alapfunkcióit tekintve a telefonálás mellett az akusztikus és vizuális rögzítés megvalósítására lett kifejlesztve, amelyen a rögzített médiatartalom gombnyomásra, vagy távoli hozzáférés engedélyezésével a világ bármely táján elérhetővé válik egy másik fogadó berendezés számára a telekommunikációs hálózatot, mint átviteli utat használva.

Továbbá a rádiótechnika és a számítástechnika rohamos fejlődésének köszönhetően távolról detektálhatóvá és értelmezhetővé váltak az elektromos kommunikációs berendezések működéséből fakadó jelek, melyek információtartalommal bírnak. Az előzőek alapján, logikus az a megközelítés, amely szerint az adatokból nyert szenzitív információkat olyan helyiségben kell feldolgozni illetve olyan „helyiségben – tárgyalóban” kell megosztani az arra jogosultakkal, amelyben biztosított az emberi kommunikációk védelme a bizalmasság biztosítása érdekében. A kommunikáció különböző formáiból eredő és a járulékosan megjelenő információt hordozó fizikai jelenségek a védett tér körülhatároló falainak síkjában, meg kell hogy álljanak. A biztonságot és annak fenntartását a megjelenő információ értékével arányos határok között, – a ma használatban lévő vagyonvédelmi és a villamos méréstechnikai, elektrotechnikai eszközökkel – biztosítható formában szavatolhatóan kell kialakítani.

1.2.1 Biztonsági rés meghatározása

A hagyományos munkaszervezésben az adatok és információk feldolgozásának folyamata, valamint az azokból nyert eredmények, információk, gyakran hangzanak el élő szóban, vagy jelennek meg vizuálisan személyes megbeszéléseken. Ezzel egy újabb információ tartalmú fizikai megjelenési közeget létrehozva, ahol az információ, természetes közegében az ember számára direkt módon a legkönnyebben megérthető formában fordul elő. Feltevésem szerint az eddigi előzetes kutatásaim eredményeit figyelembe véve, ma Magyarországon nincs megfelelő definiált intézkedés az érzékeny (esetenként minősített) adatok szóbeli tárgyalási helyszínének kialakítására, valamint definiált műszaki leírás egy megfelelő védett helyiség megalkotására, egyenszilárdsági aszimmetriát okozva az információ biztonságának megjelenési szintjei között.

Ebből a megállapításból fakadóan kutatom az elhangzott szó és vizuális információ tartalmának fizikai védelmére vonatkozó megoldásokat.

1.3. Védett helyiségek

A védett helyiségek kialakításának meghatározása, mindig a megoldani kívánt védelmi célként kell, hogy megvalósuljon. Példákat állítva válik egyértelművé a téma szempontjából tárgyalt védett helyiség mechanizmusának megértése, mert a következőkben láthatjuk, hogy számtalan alapkövetelményt állíthatunk egy ilyen helyiséggel kapcsolatban.

Klasszikus esetben a védett helyiségben a fizikailag megfogható értéktárgy biztonságba helyezése a cél. Az ilyen helyiség tipikusan a bankokban található széf. Továbbá feladata lehet az átjutás elleni védelem megalkotása is. Más megközelítésben védett helyiség kialakítható a természet elemi ereje ellen is, főként az amerikai kontinensen találhatunk ilyen helyiségeket a nagy erejű szélviharok elleni védelemre kialakítva. A témához közeledve ismert a katonaság, valamint a polgári védelem által létrehozott védett objektumok és óvóhelyek létezése is, amely szintén a védett helyiség kategóriába sorolható, és itt szintén elsősorban a fizikai védelem kialakítása a cél, az emberi szervezetet károsító, pusztító hatásokkal szemben. Itt már követelmény lehet a stabil kommunikációs rendszer kiépítése, valamint ellentevékenység indítására alkalmas helyiség megalkotása. Védett helyiségről beszélhetünk a fizikai, biológiai kutató intézmények esetén is, amikor különböző, a kutatás tárgyát képező káros

hatásoktól kell megóvni a kutatók, valamint a környezet épségét, vagy épp a külső szennyeződésektől kell megóvni a vizsgált folyamatot.

A téma szempontjából a fent leírtak alapján az említett információbiztonsági egyenszilárdság kialakítása az elérni kívánt cél, az információ humán közeli megjelenési formájának védelme érdekében, a bizalmasság megteremtése tekintetében.

1.3.1 A téma szempontjából mérvadó védett helyiség meghatározása saját elgondolás alapján

A téma szempontjából a védett helyiség fogalmát meghatározva, az olyan elhatárolt térrészt nevezünk védett helyiségnek: ahol érzékeny, értékkel bíró adatok és információk, minősített adatok és információk jelennek meg, az ember számára közvetlenül értelmezhető fizikai formában (akusztikus és vizuális módon). A megvalósítani kívánt cél az, hogy azok az adatok és információk, amelyek ebben a védett helyiségben előállnak, megjelennek, emberi kommunikáció során interaktust alkotnak, azok illetéktelen számára ne legyenek hozzáférhetőek, valamint azok jogosulatlan fél általi megszerzése, ne legyen lehetséges, se közvetlen, se közvetett, se technikai módon. Cél egy egységes védelmi szilárdságú térrész kialakítása, és annak fenntartása. A kommunikáció különböző formáiból eredő és a járulékosan megjelenő információt hordozó fizikai jelenségeknek a védett tér körülhatároló falainak síkjában meg kell, hogy álljanak. A határoló falazaton túl, a helyiségben létrejött információval korreláló fizikai jelenségek terjedéséből, a helyiségben előálló információ ne legyen megismerhető.

Az ilyen helyiséget saját elnevezés alapján, a – védett helyiség – elnevezésen túl "Komplex Védett Tárgyaló - KVT" elnevezéssel nevezném meg.

A kutatásban a – védett helyiség – elnevezést használom.

ÖSSZEGZÉS

Összegezve jelen fejezetben kifejtettem az adat és az abból nyerhető információ elméleti összefüggését. Következtetésként levonható, hogy ahhoz, hogy egy adat az ember számára értelmezhető legyen, egy algoritmus alapján fel kell azt dolgoznia. Az összefüggés alapján bemutatom az információs architektúrát piramis modell alapján, amely bemutatja a hatalom és a tudás kontextusát, a feldolgozott adatból nyert információ szemszögéből. Összefüggést találok az információ és annak értéke között, amely a döntési bizonytalanság mértékével párosul. A fejezet céljaként teljesítve összegzem a felmerülő információbiztonsági probléma hátterét és fókuszt állítok a kutatás további irányára. Csoportosítom a kommunikáció védett és megjelenő elemeit. Ez a csoportosítás a későbbiek során meghatározó lesz a védett helyiségek modelljének kialakításához. Eredményként megjelenítem a védelmi intézkedésekkel ellátott információ forrásait, a kommunikációs interfészeket, a megjelenő védeni kívánt fizikai hatásokat felsorolva. Az információ védelme érdekében legyen az minősített vagy szenzitív, több kritériumot kell teljesíteni. Nem sérülhet az adat bizalmassága, sértetlensége, hitelessége, rendelkezésre állása, mely indokolja a védelem szükségességét és arányosságát.

Új tudományos eredményként megfogalmaztam a téma szempontjából releváns biztonsági rés, és a téma szempontjából mérvadó védett helyiség fogalmát. Megállapítást nyert, hogy a kutatás szempontjából az információbiztonságot érintő probléma fennáll, így az előzetes elemzéseim okfejtései megfelelőek.

II. VÉDETT HELYISÉG KIALAKÍTÁSÁNAK RELEVANCIÁJA

Jelen fejezet célja a második hipotézispontom igazolása. Feltételezésem szerint az előző fejezetben meghatározott védett helyiség kialakítása, meghatározott intézményekben indokolható, ahol a helyiség használata a társadalomra és gazdaságra pozitív hatással van. Az elhangzott szó védelme érdekében a törvényi oldalt megvizsgálva, műszaki tartalom és előírások után kutattam.

BEVEZETÉS

A téma aktualitását bizonyítva, jelen fejezet első részében áttekintem a kutatás időpontjában hatályban lévő forrásokat, a kutatási téma szempontjából meghatározó magyar törvényi szabályozókat. Megvizsgálom, hogy a jogalkotó részéről a kutatás témáját felölelő, elhangzott szó és megjelenő vizuális tartalom, valamint a kommunikáció során megjelenő információ tartalmú fizikai jelenségek védelme szempontjából, milyen mértékben vannak érvényben műszaki védelmi intézkedések és előírások. Definiáltak-e, létezik-e hazai jogi keretrendszer, vagy valamely területet meghatározó jogszabályi előírás a kutatás céljául kitűzött védett helyiség kialakítására vonatkozólag.

A fejezet második részében áttekintem a védett helyiségek kialakításának mérvadó indokait az információ értékének függvényében. Foglalkozom a kockázatelemzés alapvető fogalmi meghatározásaival a védett helyiségek létesítési igényének meghatározására. A létfontosságú rendszerek felsorolásával áttekintem az ajánlott szektorok létesítményeinek megnevezését a „védett helyiség" ajánlott kialakításának elhelyezése kapcsán, az ágazatok megnevezésével. (Lásd később kibontva 2.4 fejezetben.) Korunk információs rendszerei, valamint infrastruktúrái nélkülözhetetlenek lettek a társadalom számára. Az emberek élete, még ha nem is tudják, a védett helyiségek üzemeltetése kapcsán válik biztonságosabbá. A fenntartó és jóléti rendszerek magukba integrálták az információs rendszerek elemeit, ezáltal teljes infrastruktúrát kialakítva. Az infrastruktúrák tervezése és üzeme stratégiai fontosságú lett. Bármilyen infrastruktúrát is tekintünk, a védelem elvi és fizikai kialakítása összetett mérnöki feladat, amely átfogóan szinte az összes műszaki szakágat érinti. Egy ilyen infrastruktúrához általában lokálisan kötődik valamilyen védett helyiség kialakítása is. Az ilyen helyiség, nem csak technológiák védelmére szolgálhat, hanem a téma alapján az ember-ember közötti kommunikáció információbiztonságára is. Egy létfontosságú

infrastruktúra működését a biztonság megteremtése alapvetően befolyásolja, így a társadalom számára is érdek a megfelelő kialakítás. A kialakítani kívánt rendszer vagyonvédelmi, információbiztonsági és a hálózati elemek komplex védelme szempontjából is meg kell, hogy feleljen arányos mértékű biztonsági és védelmi követelményeknek. Ezek elengedhetetlenek az emberek jólétének biztosítása érdekében. A társadalmi viszonyok rendezésének és a műszaki szabványok általános érvényesülésének egyik fontos eszköze a jogi szabályozás, ezért szükséges a jogi környezet témához illeszkedő részeinek áttekintése, valamint illeszkedési rések felfedezése esetén megoldási javaslat felvetése.

2.1 Törvényi szabályozók, áttekintés

Az információbiztonság megteremtésének törvényi oldala főként a titokvédelemhez és a minősített adatok védelméhez kapcsolódik, amely egy különleges terület. A törvényalkotó deklarálja a személyiségi jogokat, valamint törvények és rendeletek létrehozásával, helyi szintű utasításokkal védi az információk bizalmasságát. Az információk védelme több elvi megközelítés alapján történik. [5]

A kutatási területnek megfelelő irányt választva ketté kell bontani a biztonság megteremtéséhez szükséges intézkedéseket. Az egyik az emberi tényező, a másik a technikai szint.

Az emberi szintű információvédelem, külön kutatási terület, azonban az információk védelme törvénnyel, valamint különböző egyéni vállalásokkal, szerződésekkel erősíthető. [25]

Az információbiztonság kialakítása során az adat titkosságának megóvását, bizalmasságát, rendelkezésre állását, sértetlenségét és hitelességét kell megőrizni. Mind az állami- és a magánszektorban is az érdekelt fél, felek közötti bizalmas és számukra érzékeny jellegű adatok védelmét kell megvalósítani. A fő különbség az állami és magánszektor között, hogy míg egy állami szerv, vagy hivatal, vagy az azokkal szerződésbe bevont, kapcsolatban álló civil társaság törvény által kötelezett a minősített és érzékeny információk védelmére, a tisztán magánszférában a saját érdek védelme a mozgatórugója az információvédelemnek. A jogszabályi környezet vizsgálatának célja, hogy a jogi források áttekintése alapján, igazoljam a kutatás aktualitását. Teljességében nem elérhető meghatározott műszaki ajánlás, a téma szempontjából mérvadó védett helyiség kialakításra. A védett helyiségek kialakítására vonatkozólag, az ember-ember

közötti közvetlen kommunikáció védelmére irányuló, a kommunikációs környezet kialakítására vonatkozó tartalmakat kutatva a következő szabályozókat tekintettem át.
A titok védelmének témakörében elsőként, az információbiztonság megteremtésének alapvető kiindulópontjaként, a Polgári Törvénykönyvről szóló (Ptk.) 2013. évi V. törvényt (Ptk.) tekintettem át, amely alapot biztosít a titokhoz való jog megteremtésében. A törvény harmadik része a személyiségi jogokat tárgyalja, melynek a 2:42. § alapján rendelkezik a személyiségi jogok általános védelmére, illetve a 2:46. § rendelkezik a magántitokhoz való jogról. [26] A törvény alapvetően a személyek alapvető vagyoni és személyi viszonyait szabályozza, a kutatás szempontjából műszaki tartalom nem kerül meghatározásra.
Az ember-ember közötti közvetlen kommunikáció technikai védelmére irányuló kutatást folytatva, áttekintettem a törvényi szabályozók további jogforrásait, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt (Infotv.) és a minősített adat védelméről szóló 2009. évi CLV. törvényt (Mavtv.).

Az Infotv. célja „a hatálya alá tartozó tárgykörökben az adatok kezelésére vonatkozó alapvető szabályok meghatározása annak érdekében, hogy a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák, valamint a közügyek átláthatósága a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő jog érvényesítésével megvalósuljon", amely mindenkire vonatkozik. [27] Az Infotv. tartalmazza az adatok kezelésére vonatkozó keretszabályokat is. A törvényben a kutatási téma szempontjából mérvadó, az ember-ember közötti kommunikáció során megjelenő, akusztikus és vizuális tartalom védelme érdekében, a kommunikáció helyszínén alkalmazható védelmi jellegű műszaki intézkedés nem kerül meghatározásra.

A Mavtv. az Országgyűlés az állami és a közfeladatok ellátásának biztosítása érdekében, a közérdekű adatok megismerésének alkotmányos jogából, illetve e jog kizárólag szükséges és arányos mértékű korlátozásának lehetőségéből kiindulva, a minősített adat védelméről szól. Tartalmát tekintve meghatározza a minősített adat témakörrel kapcsolatos általános rendelkezéseket, a minősítők és a minősítések szabályait, a minősített adat biztonságára vonatkozó általános szabályokat, meghatározza a minősített adat védelmét ellátó szervezeteket és személyeket. A törvény célja, hogy „az alapvető jogok tiszteletben tartása, Magyarország érdekeinek védelme és az állam nemzetközi kötelezettségvállalásainak teljesítése érdekében az információs önrendelkezési jogról és az információszabadságról szóló törvénnyel összhangban

meghatározza a minősített adat létrejöttével és kezelésével kapcsolatos alapvető rendelkezéseket, a minősítési eljárás és a nemzeti minősített adat felülvizsgálatának rendjét, a minősített adat védelmének általános szabályait, a telephelyi iparbiztonság rendszerének főbb elemeit, és rendelkezzen a minősített adat védelmét ellátó szervekről és személyekről." [28]

- A törvény felsorolja azokat a közérdekeket, melyek minősítéssel védhetők.
- Kármérték alapján meghatározza a minősítési szinteket amelyek a: „Korlátozott terjesztésű!”, „Bizalmas!”, „Titkos!”, „Szigorúan titkos!”
- Keretrendszert alkot a nemzeti és külföldi minősített adatok kezelésére vonatkozóan.

E törvény tartalmazza a minősített adat védelmének szabályait. Maga a törvény az ember-ember közötti kommunikáció során megjelenő akusztikus és vizuális tartalom környezetének védelme érdekében nem ad egyértelmű technikai utasítást, azonban a végrehajtási rendeletei támpontot nyújthatnak a védett helyiség kialakításához, a minősített adat tárolásának környezeti jellemzői meghatározása során.

A következő a témában áttekintett törvény az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény. (Ibtv.)

Az Ibtv. feladata, a nemzet érdekében kiemelten fontos - napjaink információs társadalmát érő fenyegetések miatt - a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága. Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme. [29]

A kutatás során megvizsgáltam a törvény végrehajtási rendeleteit melyek a következőek:

- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet [30]
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló

törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet [31]

- az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Kormányrendelet [32]
- a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenység vizsgálat lefolytatásának szabályairól 185/2015. (VII. 13.) Kormányrendelet [33]

A rendeletek elemzése során, szorosan a kutatási témához kapcsolódó, a védett helyiség fizikai kialakításra vonatkozó rendelkezést nem találtam.

A Mavtv. végrehajtását elrendelő kormányrendeleteket áttekintve a minősített adat szempontjából, a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) kormányrendelet áttekintve [34] a rendelet az elektronikus biztonsági követelmény rendszernek a meghatározó elemeit tartalmazza. Ezen követelményelemek megteremtése szükséges a minősített adatok elektronikus kezeléséhez. A rendelet alapján a Nemzeti Biztonsági Felügyelet (NBF) ellátja a TEMPEST-re (kompromittáló kisugárzásra) vonatkozó hatósági funkciókat. A rendelet szabályozza a rejtjeltevékenységet, de a jogszabály ezen része a kutatás témája szempontjából, csak a védett helyiség kapcsán esetlegesen elhelyezett rejtjelező eszköz esetén lenne mérvadó, a kutatási téma iránya szempontjából, nem ad egyértelmű megoldást.

A következő áttekintendő kormányrendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) kormányrendelet. A 92-es kormányrendelet az információbiztonság szempontjából kiemelt jelentőséggel bíró jogszabály. Elsősorban annak a folyamatnak a részletes szabályozását találhatjuk meg benne, melynek során a gazdálkodó szervezetek telephely biztonsági tanúsítványt szerezhetnek, ezzel „Minősített szerződésbe vont gazdálkodó szervezet" kritériumot teljesítve. [35] A rendelet a kutatás szempontjából vizsgált védett helyiség kialakításához nem ad megoldást.

A kutatás szempontjából egyedülállóan, a minősített adatok kezelésére vonatkozó jogforrások közül a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010 (III. 26.) Kormányrendelet adhat részinformációkat a védett helyiség kialakításának alapvető paramétereihez. A rendelet meghatározza azon fizikai, adminisztratív és személyi biztonsági követelményrendszert, melynek kialakítása a minősített adatok kezeléséhez, azaz az adatkezelési engedély megszerzéséhez szükséges.

A rendelet támpontot nyújt a kutatás egyik fontos elemének, amely a minősített adat szóbeli megjelenésének védelme érdekében került megfogalmazásra.

A 90/2010. (III. 26.) kormány rendelet, 59. § (2) bekezdés szerint a minősített adatot kezelő szerv vezetője biztosítja, hogy azok a biztonsági területek, ahol „Titkos!" vagy ennél magasabb minősítési szintű minősített adatokról rendszeresen tárgyalnak, lehallgatás mentesek legyenek. [36]

Az elhangzott szó védelmében a kormányrendelet szintén csak a minősített adat témaköréhez kapcsolható és szó szoros értelemben csak a „Titkos!"vagy magasabb minősítési szinttől határoz meg utasítást. Azonban a rendelet nem határoz meg utasítást az ember-ember közötti közvetlen kommunikáció során elhangzott szó és megjelenő vizuális tartalom védelme szempontjából mérvadó, a fizikai környezet ilyen jellegű speciális kialakítására és ellentevékenység végzésének technikai utasítására.

Továbbá a rendelet értelmező rendelkezések fejezete definiálja az elektronikai felületvédelem meghatározását valamint az V. fejezete Fizikai Biztonság címmel meghatározza a minősített adat fizikai biztonsági alapelveit és követelményeit.

A 16. § (1) alapján a minősített adat felhasználására és tárolására szolgáló helyszín fizikai biztonsági rendszere több egymásra épülő elemből áll. Tároló rendszerek jellemzőire tesz utasítást. A fizikai biztonság külső elemei a védendő terület határait biztosítják. A fizikai biztonság közbenső elemei észlelik az illetéktelen behatolást és riasztják a reagáló erőt. A fizikai biztonság belső elemei a reagáló erő megérkezéséig késleltetik az illetéktelen behatolót a minősített adatokhoz történő hozzáférésben.

Tehát a minősített adat védelme érdekében, több egymásra épülő rendszer kerül kialakításra, azonban elsődlegesen az illetéktelen behatolás megakadályozása, valamint a reagáló erők értesítése, a fizikai biztonság megfelelő kialakítása a feladata. A rendelet I. és II. osztályú biztonsági terület helyszínének fizikai kialakítását határozza meg, amely kialakítási előírások jó alapul szolgálhatnak a védett helyiség alapvető kialakításához. A rendelet meghatároz falvastagságokat, rácsszerkezeteket, nyílászárók

esetén áttörés gátlási értéket, azonban az utasítások a téma szempontjából mérvadó, az ember-ember közötti kommunikáció során létrejövő, akusztikus és vizuális, információ tartalmú fizikai jelenségek terjedésének, megfigyelhetőségének nem teremtenek egyértelmű akadályt.

Ennek alapján a disszertáció V. fejezet kutatási eredményeit a törvényalkotó figyelmébe ajánlom a rendelet kiegészítésére, a védett helyiség alkalmazására, valamint a lehallgatás mentes környezet megteremtésére vonatkozó javasolt tevékenységek elvégzésének meghatározásához.

A magánszektorban szintén az értékkel rendelkező adatok, információk megóvása a cél viszont más jellegű háttérrel. A különbség az, hogy míg egy állami szerv, vagy hivatal, illetve az azokkal kapcsolatban álló civil cég törvény által kötelezett a minősített adatok védelmére, illetve az informatikai információbiztonság megteremtésére, úgy tisztán a magán szférában és üzleti szférában a saját érdek védelme a mozgatórugója az információbiztonság kialakításának.

A magáncégek esetében az adatbiztonság és információvédelem sokszor az adatgazda szakértelmén, valamint az anyagi lehetőségein múlik. A civil szféra törvényi védelmét a magántitokról és az üzleti titokról szóló jogszabályok alkotják. A téma vizsgálatát folytatva a kutatás szempontjából a következő jogi forrásokat vizsgáltam meg:

- a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló 1996. évi LVII. törvény. Jelen törvény tiltja az üzleti titok tisztességtelen módon való megszerzését vagy felhasználását, jogosulatlanul mással való közlését, vagy nyilvánosságra hozatalát [37]
- az üzleti titok védelméről szóló 2018. évi LIV. törvény [38]
- a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény [39]
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [27]

Az üzleti titok védelme érdekében az egyén szempontjából további törvényi kötelezettségek állnak fenn, amelyet a munka törvénykönyvéről szóló a 2012. évi I. törvény 8. § (1) és (4) bekezdései határoznak meg. [40]

A jog a titok védelemének hazai szabályozására eszközeként büntető jogi rendelkezéseket határoz meg Büntető Törvénykönyvről szóló 2012. évi C. törvényben (Btk.). A Btk. több olyan magatartást minősít bűncselekménynek, amely valamilyen

titoknak egy jogosulatlan általi megismerésére irányul. Így bűncselekménynek nevesíti többek között a kémkedés, a minősített adattal visszaélés, a gazdasági titok megsértése, az üzleti titok megsértése, a tiltott adatszerzés és az információs rendszer, vagy adat megsértése tényállásokban megfogalmazott magatartásokat. [21] [14] [41] [11] [42]
A szabályzó környezet feldolgozása során megállapítom, hogy műszaki előírások tekintetében a jogi előírások túlnyomó részt, az állami szférában, vagy azzal kapcsolatban álló szervezetek számára írnak elő, a minősített adathoz kapcsolható műszaki követelményrendszert. A civil szféra szenzitív adatainak védelme műszaki utasításokkal kevésbé lefedett terület. Összegezve a témához kapcsolódó jogszabályi háttér áttekintését követően a 90/2010 (III.26.) kormányrendelet, a minősített adatra vonatkozó technikai utasításainak figyelembe vételén kívül, - a kutatási téma szemszögéből előírt, az ember-ember közötti kommunikáció során akusztikusan és vizuálisan megjelenő információ fizikai védelmére vonatkozó speciális kialakítására, a kutatás során a későbbiekben vizsgált, az információbiztonságot fenyegető technikai lehetőségek kivédésére alkalmazható műszaki előírást - nem találtam.

2.2 A biztonság és a védelem kapcsolata

A kutatás szempontjából szükséges tisztázni a biztonság és védelem kifejezések jelentését, mivel a védett helyiségek kapcsán védelmi intézkedések sorát célszerű kialakítani az információ biztonsága érdekében.
A magyar nyelvben a „védelem" szó tevékenységet, illetve tevékenységeket [10] [34] [111] jelent, amelynek célja, hogy egy bizonyos szinten tartsa vagy erősítse azt az állapotot, amelyet, biztonságosnak nevezünk. A „biztonság" egy állapot, amely valakinek, vagy valaminek a jellemzője.
A védelmi tevékenységet egyszerűsítve „támadó és védő” személyesíti meg, melynek során a támadó cselekedete egy védett érték irányába mutató tevékenységre irányul. A tevékenység során a védő a védeni kívánt értéket védi, elhárítja a támadásokat. A támadás valamilyen útvonalon zajlik le, melyek ellen védelmi akadályokat, intézkedésekkel kell tenni. A játékelméleti megfogalmazás szerint az ilyen játékot „kétszemélyes, nullától különböző összegű" játéknak hívják. Két fél játéka esetén a támadó nyeresége sohasem egyenlíti ki a védő veszteségét. A védő fél vesztesége a védelmi intézkedésekre fordított költsége amihez hozzáadódik a támadások során védeni kívánt érték, valamint a védelmi rendszer fenntartási költsége, nyereség nélkül. A

támadó kára a támadás költsége, beleszámítva a védő által, a támadó számára okozott költséget a támadás során. A támadó nyeresége a megszerezni kívánt értékig terjed, amely jelen kutatás kontextusában az információ. A védő olyan védelmi intézkedéseket hoz, hogy a sikeres támadás valószínűségét csökkentse. A védelmi intézkedések kialakítása a támadás költségeit is növeli. A teljes biztonság kialakítása során szükséges, hogy a védelmi intézkedések sora, minden fenyegetésre valamilyen védelmi megoldást adjon, a támadási pontokon akadályt teremtsen a támadó számára. A védett helyiségek szempontjából teljes körű, zárt, folytonos és a kockázatokkal arányos védelmet szükséges megvalósítani. A védelem teljeskörűsége alatt azt értjük, hogy a védelem kialakítására hozott intézkedések a védeni kívánt rendszer minden elemére kiterjednek. A védelem zártságáról beszélünk, ha az összes meghatározható fenyegetést figyelembe vesszük. A védelem folytonossága során az időben változó körülmények és viszonyok ellenére is megszakítás nélkül kell megvalósulnia a védelemnek. A kockázattal arányos védelem alatt azt értjük, hogy a védelemre fordított költségek arányosak a várható kár mértékével. [25] [10] [34] [111]

A kockázat felírása képlettel is definiálható, amelyet az 1. számú képlet fejez ki:

$$r = \sum_{t \in T}(\mathrm{dt} x \mathrm{pt}) \qquad (1)$$

ahol:
r: a kockázat [Ft/év],
T: a releváns fenyegetések halmaza,
dt: egy adott kockázat bekövetkezéséből származó kár [Ft],
pt: egy, a fenyegetettség által okozott kár bekövetkezésének várható éves gyakorisága [1/év].
(Forrás: [43] 10. oldal)

A fenyegetettség mértéke a fenyegetettség bekövetkezésének gyakoriságától, és az okozott kár nagyságának mértékétől függ. A kockázat arányosságának értelmezése során elmondható, hogy az „elmaradt kár haszon"-ként értékelhető. Következtetésként levonható, hogy a védelem kialakítására szánt beruházás hasznot hoz. [43]

2.3 A védett helyiség kialakításának szükségessége a kockázat függvényében

A védett helyiségek kialakításának szükségességét a felmerülő, az információ biztonságát fenyegető kockázatok felmérése alapján értékelhetjük. A védett helyiségek kialakításának igénye esetén, mindenképpen szükséges egy audit elvégzése, amely az információbiztonság pillanatnyi állapotának kockázatait méri fel, a lehetséges bekövetkező sérülékenység függvényében. A biztonsági audit során a vizsgált rendszert elemeire bontjuk, és külön megvizsgáljuk azokat a rájuk ható tényezők függvényében.

A védett helyiségek szükségességének megállapításakor a megjelenő információ tartalmú fizikai jelenségek fizikai biztonságának elemzése során felmerülő kockázatot kell szem előtt tartanunk.

A kockázatelemzés egy olyan folyamat, amely során felmérjük a rendszert károsan befolyásoló veszélyeket és a védelmi lehetőségeket abból a szempontból határozzuk meg, hogy az információbiztonság a megfelelő szintet érjen el. Védett helyiségek esetén a kockázatot kiváltképp a technikai hírszerzés vonatkozó eszközrendszerének alkalmazhatósága tekintetében vizsgáljuk. A kockázatelemzés egy esemény, vagy folyamat következményeinek negatív értékelése, a bekövetkezés valószínűségének és a következmény súlyosságának a figyelembevételével. A kockázatelemzés során a cél az arányos védelem kialakítása. Jelen esetben minden, az információ biztonságát fenyegető veszélyt vagy tényezőt kockázatnak nevezünk. A kockázat valamilyen folyamat, esemény vagy cselekvés következményeként létrejövő veszteség vagy károsodás lehetőségének a mértéke.

A kockázatok elemzése során két fő kockázatelemzési felosztást különböztetünk meg, melyek a valószínűségi alapú és a determinisztikus alapú megközelítések.

A valószínűségi megközelítés során a kockázat szintje nem csökkenthető nullára, matematikai számítások alapján meghatározható egy kockázati szint.

A determinisztikus megközelítés alapján a kockázatok nullára csökkentése a cél. A kockázati veszélyek feltárásán túl a kockázat csökkentésére vonatkozó intézkedéseket, védelmi rendszereket és feltételeket szükséges ellenőrizni az események és a következmények elemzésével együtt, a bekövetkezés valószínűségének számítása nélkül. A védelem megteremtése során a károk bekövetkezésének százszázalékos kizárása jelentős költséget eredményez. A kialakítás tekintetében azokat a helyeket érdemes így kialakítani, ahol az információ biztonságának sérülése elvileg sem megengedhető, illetve az alacsony információbiztonsági veszélyeztetettséget jelentő kockázat is elkerülendő.

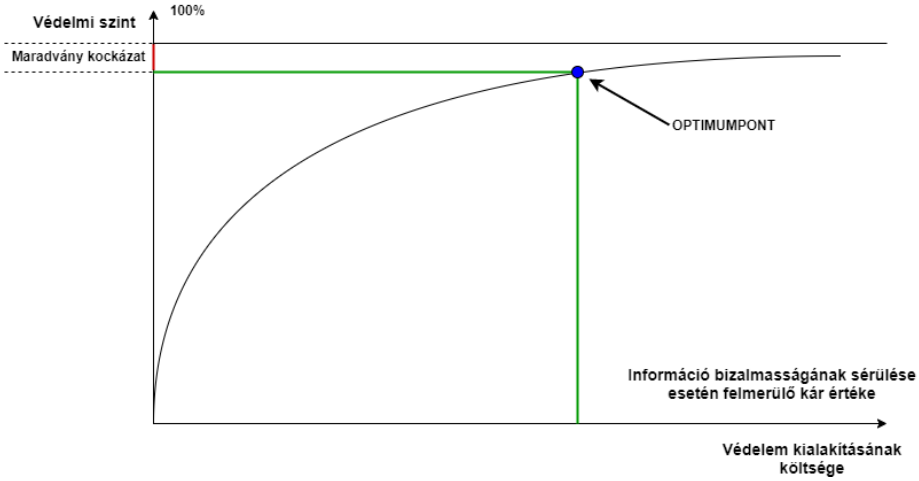
A kockázatelemzés valószínűség alapú szemléletét tekintve további három elméleti megközelítésre bontható, melyek a kvalitatív, a kvázi-kvantitatív és a kvantitatív módszerek.

Kvalitatív (minőségi) módszer esetén a káresemény bekövetkezését a gyakoriság figyelembevételével és a következmény együtt történő értékelésével vizsgálják.

Kvázi-kvantitatív módszer esetén, amennyiben a valószínűség és a következmény számszerűen nem ismert, akkor a kár mértéke becsült adatokkal adható.

Kvantitatív (mennyiségi) módszer szerint, ha az esemény bekövetkezésének a valószínűsége és a következményként megjelenő kár összege számszerűsíthető, akkor a kockázat számszerűen megadható a káresemény összegének és a bekövetkezés valószínűségének szorzataként. [43] [44] [45] [46]

Véleményem szerint a védett helyiségek kialakítása során a kockázatok csökkentése és az optimális védelem kialakítása egy optimális ponton behatárolható, amely függ a védett helyiség használójának közigazgatási, gazdasági és piaci szektorban betöltött pozíciójától, amelyet a szektorban mért gazdasági forgalom, vagy a keletkező védett információ értéke határoz meg.



3. ábra Optimum pont a vagyonvédelem kialakításának költsége és a maradványkockázat összefüggésének kialakítása [47]
Forrás: saját szerkesztés

A 3. számú ábrán az optimum pont látható, amely egyrészről a védelem kialakításának költségarányát szemlélteti a védelem szintjének százalékos dimenziójával, másrészről a koordináta-rendszer dimenzióinak váltása esetén a maradvány kockázat mértéke és az információ sérülése esetén felmerülő kár értéke szemszögéből.

Az ábráról szemléletesen leolvasható, hogy egy bizonyos szint fölött ha az optimum pontot pozitív irányban vízszintesen elmozgatjuk, úgy a védelem kialakításának költségei jelentősen nőnek, a függőleges tengelyen lévő védelem szint is közelíti a száz százalékot, a maradvány kockázat ellenben kismértékben csökken. [48] [45]

2.4 A védett helyiségek kialakításának lehetőségei, a kapcsolódó szektorok, létfontosságú és információs infrastruktúrák

Elképzelésem alapján a védett helyiségek kialakítása kapcsán, ajánlások tekintetében meg kell jelölni azokat a szegmenseket, ahol érdemes kialakítani a kutatás tárgyának

megfelelő védett helyiséget. Az ajánlott szektorokra jellemzően a keletkező információk egyenkénti értéke is jelentős mértéket képviselhet. [49]

A kutatásom alapján az ágazatok szereplői jellemzően állami, vagy „Minősített szerződésbe vont gazdálkodó szervezet" magánszektor szereplők, azonban tisztán a magánszektorban működő szereplők is érdekeltek lehetnek védett helyiség kialakításában. A kialakítás szükségességének alapja a szenzitív adatok értékének függvénye, amennyiben az egyáltalán megbecsülhető. Az ágazatokban megjelenő információ védelme mind gazdasági, mind társadalmi szempontból jelentős lehet. Ha közszolgáltatói infrastruktúráról van szó, akkor a társadalom szempontjából is fontos az infrastruktúra működése, ezzel nehezen megbecsülhető értéket teremtve az ágazatban megjelenő információnak. A működőképesség megbénulása jelentős szolgáltatás kieséssel, valamint kárral járhat, nem csak a létesítő és fenntartó számára, hanem a felhasználó csoportok számára is. [50]

A kiemelt intézményeket fontosságuk rangsorolásával és a kiesésük miatt okozott kár mértéke szempontjából, továbbá a betöltött funkcióik szerint, az ilyen infrastruktúrákat és ezzel együtt az ilyen infrastruktúra információs rendszereit kritikus infrastruktúra megjelöléssel láthatjuk el. Európai Uniós jogalkotás 2016. július 06-án megjelent -Az Európai Parlament és a Tanács (EU) 2016/1148 - A hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelve, amely NIS irányelv elnevezéssel is ismert. A megjelent irányelv II. melléklete tartalmazza azoknak az alapvető szolgáltatásokat nyújtó szereplőknek a listáját, akik ilyen csoportba tartoznak. Az irányelvnek megfelelően a magyar jogrendbe illesztett megfelelője a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, ahol a létfontosságú rendszerek megnevezését a törvény 1. számú melléklete tartalmazza. [51] [52] [53] Létfontosságú rendszerek azok, amely szervezetek a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújtanak, akiknek az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ, és az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában. [54] [55] [56]

Az ágazatok a következők:

- Energia
    - Villamos energia
    - Kőolaj
    - Földgáz
- Közlekedés
    - Légi közlekedés
    - Vasúti közlekedés
    - Vízi közlekedés
    - Közúti közlekedés
- Banki szolgáltatások
- Pénzügy
- Agrárgazdaság
- Egészségügy
- Társadalombiztosítás
- Víz - vízellátás és elosztás
- Digitális infrastruktúra
- Honvédelem
- Közbiztonság-védelem

Egy-egy példát kiemelve, a létfontosságú infrastruktúrák pénzügyi forgalmát szemügyre véve, látható a jelentős árbevétel mértéke, mely véleményem szerint indokolttá teszi a védett helyiség kialakítását.

Energia ágazat:
MOL Nyrt. - Nettó árbevétele 5168,7 milliárd forint (2018)[1]

Közlekedés ágazat:
MÁV- csoport - Nettó árbevétel 15,6 milliárd forint (2019)[2]

Banki szolgáltatások ágazat:
OTP Bank Nyrt. - Nettó árbevétel 321,2 milliárd forint (2020)[3]

Digitális infrastruktúra ágazat:
T-Systems Magyarország Zrt. - Nettó árbevétel 85,5 milliárd forint (2020)[4]

A fentiek alapján szükségesnek tartom az állami és magánszektorban a védett helyiségek kialakítását. Továbbá kiemelt fontossággal javaslom a védelmi funkciót ellátó ágazatok

[1] https://ado.hu/cegvilag/jo-evet-zart-a-mol/
[2] https://infostart.hu/gazdasag/2020/06/03/nyereseges-lett-a-mav-csoport
[3] https://www.ceginformacio.hu/cr9310007548
[4] https://www.ceginformacio.hu/cr9310000747

létesítményeit illetően is, amelyek az esetlegesen előforduló felbecsülhetetlen bizalmasságú információk megjelenésének feltételezése alapján kiemelt fontosságúak.
Az állami szektor tekintetében a védett helyiségek szükségessége, a minősített adat humán információmegosztó környezetében kiemelt jelentőségű lehet, mivel a minősítési szintek és az azok sérelmével jellemezhető kár mértéke jelentős kockázati tényezőt hordozhat magában. A jogi szabályozók kutatása során a „Titkos" vagy magasabb minősítésű információmegosztói környezetben kommunikációs interraktusok alkalmával jogszabályi előírás a „Lehallgatásmentes" környezet, ezáltal az ilyen minősítési szintű információkat megosztó és feldolgozó környezetekben, egységesen szervezetenként indokolt védett helyiség kialakítása. [57]; [48] [58]
A szenzitív adatok védelmére törvényi előírásokkal nem szabályozott szektorokban, a téma szempontjából meghatározott védett helyiség kialakítása tulajdonképpen szektortól függetlenül mindenhol ajánlható, amennyiben a kialakításra szánt összeg a kockázatelemzés eredményével alátámasztható. [59] Véleményem szerint a létfontosságú rendszerek és létesítmények (kritikus infrastruktúrák) felsorolásában részvevő ágazati szereplők objektumaiban az előzőek alapján, a döntéshozói környezetben javasolt lehet védett helyiségek kialakítása, mivel a vezetői döntések információs értéke ágazatonként GDP-ben megjelenő értékkel rendelkezhet. Továbbá szintén ajánlható védett helyiség kialakítása egyéb, nem a létfontosságú rendszerek felsorolásába eső szereplők számára is, amennyiben az előálló információ értéke, valamint a kockázatelemzés eredménye megkívánja a védett helyiség kialakítását. Ebben az esetben a tulajdonosi kör, saját elhatározása alapján dönthet úgy, hogy a gazdasági társasága megérett egy ilyen helyiség kialakítására.
A felsorolás teljessége kedvéért meg kell említeni, hogy azoknak a gazdasági szereplőknek, akiknek az árbevétele, valamint az előálló információk értéke nem összemérhető a védett helyiség kialakításának és fenntartásának költségével, kevésbé javasolt ilyen helyiséget kialakítani és fenntartani, mivel az rendkívüli terhet jelentene a működtetett gazdasági társaság költségvetésére. A következő 1. számú táblázat a javaslataim összefoglalását tartalmazza a védett helyiség kialakítására.

Védett helyiség kialakítása nagyon javasolt	Védett helyiség kialakítása javasolt	Védett helyiség kialakítása javasolható	Védett helyiség kialakítása kevésbé javasolt
Állami szektor, valamint szerződésben álló vállalatok, a minősített adat védelmére	Kritikus infrastruktúrákat üzemeltető gazdasági szereplők	Jelentős információs vagyonnal rendelkező gazdasági szereplők	Nincs túl jelentős információs vagyon

1. számú táblázat Védett helység kialakításának szükségessége saját elképzelés alapján
Forrás: saját ábra

2.5 A védett helyiségek kialakítása kapcsán meghatározó tudományterületek

A téma kapcsán szóban forgó védett létesítmények és helyiségek megvalósítása tekintetében, számos tudományterület és szakma képviselteti magát, melyek kutatásom alapján felsorolva a következők:

- biztonságtudomány
- hadászat, hadbiztonság
- geológiai ismeretek és tudományok területe
- meteorológiai ismeretek
- építészet
- gépészet, gépész energetika területe
- villamos energetika
- villamos távközlés
- informatika
- fizika
- akusztika
- közgazdaság

A felsorolás alapján látható, hogy egy védett létesítmény, továbbá egy védett komplexum, helyiség milyen sok tudományterület összegzett munkájaként kerülhet kialakításra a megfelelő funkcionalitás érdekében. Az egyes tudományterületek feladatai és azok leírása külön kutatási irányt teremt, melyek terjedelmi okok miatt nem részei jelen kutatás anyagának.

ÖSSZEGZÉS

A fejezet első részében részletezem a titok és minősített adat védelmére vonatkozó törvényeket és kormányrendeleteket, amelyek definiálják a minősített adat személyi biztonságra, adminisztratív biztonságra, fizikai biztonságra, elektronikus biztonságra, hardver biztonságra és szoftverbiztonságra vonatkozó előírásait. Továbbá áttekintem a törvényi szabályzók kapcsolódó szabályzóit a témához kapcsolódó érvényben levő előírások feltérképezése érdekében.

Igazolom a hiányosságot állító feltételezésem, amely a téma szempontjából vizsgált felvetésre, az ember-ember közvetlen kommunikáció során elhangzott szó és megjelenő vizuális tartalom, továbbá a megjelenés során keletkező információ tartalmú fizikai jelenségek védelmére irányul. A kutatás idején, a Magyarországon hatályban lévő elérhető előírások tekintetében, nyílt forrásból nem elérhető a téma kontextusában mérvadó védett helyiség kialakítására, az ember-ember közötti közvetlen, szenzitív kommunikáció helyszínét meghatározó kialakítására egyértelmű utasítás. Az elérhető meghatározásokban a hagyományos értelemben vett objektumvédelem fizikai biztonságát megteremtő védelmi elemekre, az elektronikus jelzőrendszer elemeire, továbbá azok minőségi paramétereire kapunk meghatározást. Eredményként elmondható, hogy a jogforrások nem adnak egyértelmű meghatározást a témában, továbbá a jogi szabályzók értelmezése során, nem kapunk deklarált meghatározást a „Titkos" vagy magasabb minősítési szintű tárgyalások környezetének lehallgatás-mentességéről, melynek alapján a kutatás egyik eredményként a javaslat fejezetben, ajánlom az eredményeimet a vonatkozó jogszabályok kiegészítésére.

Ezt követően részletezem a védelem és a biztonság kapcsolatát, illetve a védelmi intézkedések kialakítására vonatkozó gazdasági megfontolást.

Védett helyiséget ott érdemes kialakítani, ahol a helyiség kialakítása és használata során a védett információ időhányados szerinti átlagértéke arányban van a beruházás költségével. Azaz, egy védett helyiségben, az idő folyamán elhangzó információ bizalmasságának akár csak egy alkalommal való sérülésének gazdasági vagy erkölcsi negatív értéke, összemérhető a védett helyiség kialakításának költségeivel. Hipotézisem igazolásaként meghatározom azokat a szektorokat, intézménytípusokat, ahol megfontolandó a védett helyiség kialakítása, a kutatás aktualitását erősítve. Feltételezésem megválaszolásaként védett helyiségek kialakítása javasolt az állami és magán szektorok intézményrendszereihez kapcsoltan, amelyek kritikus infrastruktúrák

intézményei, vagy kapcsolódó részei. Továbbá ajánlom a védett helyiségek kialakítását a jelentős eszmei és gazdasági információs értékkel rendelkező magánszektor szereplőire nézve is. A fejezet végén felsorolom a védett helyiségek kialakításához szükséges, meghatározó tudományterületek sorát.

III. VÉDETT HELYISÉG STRUKTÚRÁJA

Jelen fejezet célja a harmadik hipotézispontom vizsgálata. A védett helyiségek struktúráját az objektumvédelem összetevőinek felhasználásával és - a későbbiekben csoportosított- kockázati elemek kizárásával alakíthatjuk ki. A védelmi elemek a fizikai biztonság megvalósításának hagyományos rendszerét magukba kell foglalják, mivel a védett helyiségek alapvető fizikai biztonsága és elhelyezési struktúrája meghatározza a téma fókuszául választott biztonsági terület kialakításának lehetőségeit.

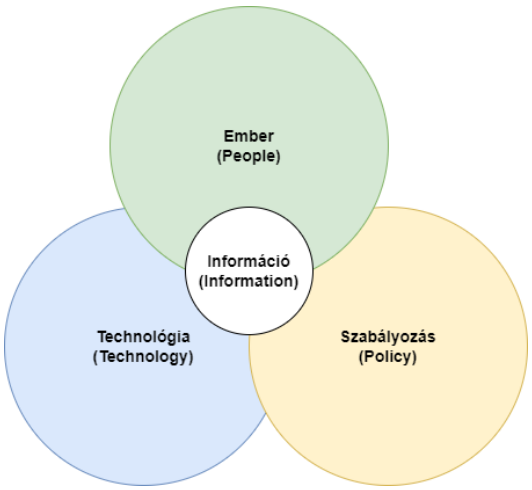
BEVEZETÉS

Az információbiztonság kialakításának feltétele az egyén, a technológia és a biztonság kialakításához köthető rezsimszabályok halmazainak hármas egysége. A kutatási téma további irányvonalát a technológia halmazába való besorolásával jelölöm ki. A védett helyiség különálló biztonsági zónaként kell, hogy kialakításra kerüljön, amely az objektumvédelem biztonságszervezése során is autonóm zónaként kell, hogy üzemeljen. A védett helyiség kiinduló állapotát és a védelem kialakításának eszközeit a hagyományos objektumvédelem eszközrendszerével teremthetjük meg. A kialakítás kapcsán meghatározom azokat a hagyományos védelmi eszközöket, és elhelyezési struktúrát amelyek felhasználásával megteremthető egy védett helyiség kialakítására alkalmas környezet. Javaslatot teszek védett helyiség objektumon belüli elhelyezésének kialakítási szempontjaira, megalapozva a védelmi intézkedések struktúráját.

3.1 Az információbiztonság PPT (People, Policy, Technology) modell, valamint a védett helyiség komplex biztonságának kutatása

A védett helyiségek információbiztonságának megteremtése kapcsán, Steven Schlarman (People, Policy, Technology, - PPT) ember, szabályozás, technológia három alkotós modellje jó megközelítést nyújt az információbiztonság elméleti megteremtése során. [60] A modell alapján a halmazok egyensúlyban tartásával alakítható ki az információbiztonság optimális mértéke az egyenszilárdság elvének megfelelően. Ennek a három halmaznak a közös pontja a biztonság állapota. Bármely halmaz csökkenése, negatív kihatással van az információ halmaz méretére, azaz az információ biztonságára. A megfelelő szint eléréséhez összhangban kell lennie az alkalmazott technológiák

szintjének a felhasználók biztonságtudatos viselkedésével, valamint a bevezetett biztonsági intézkedések, (rendszabályok) mértékével. [17] A 4. számú ábrán a PPT modell látható.



4. ábra Az információbiztonság elemei PPT modell Forrás: [60] alapján

A technikai információbiztonság megteremtése az ábra elemei közül főként egy alkotó halmazzal kapcsolható össze amely a Technológia (Technology) halmaz. A modell Ember (People) alkotó, nem igazán szabványosítható és egységesíthető fogalom. Az egyén az információbiztonság megteremtése kapcsán az információbiztonságilag tudatos viselkedés (1.2 fejezet alapján) kialakításával járulhat hozzá az információbiztonság megteremtéséhez. Ez egy tanuláson alapuló folyamat, megfelelő viselkedési normák betartásával, a biztonságtudatos viselkedés (information security awareness tanfolyamok) anyagának elsajátításával, valamint a policy-k elfogadásával erősíti a biztonság szilárdságának megteremtését. A szabályozás (Policy) halmaz az információbiztonság elvi befolyásoló intézkedéseinek összessége, amely a rezsimintézkedések, valamint a szabályozók együttesét jelenti. A szabályozók szankciói rendszerint különböző peres eljárások, felelősségre vonási intézkedések. Jelen kutatás a védett helyiségek fizikai kialakításának irányába mutat, ezért a PPT modell Ember és Szabályozás halmazainak elemei a továbbiakban csak a kutatás során felmerült mértékben kerülnek megjelenítésre. A védett helyiség kialakításának kutatása során a PPT elméleti modell elemei közül a Technológiai halmaz a további fő irány, amely mértéke dominál az ember és szabályozás halmazelemekhez mérten.

3.2 Az objektumvédelem hagyományos elemeinek felhasználása a védett helyiségek kialakítása kapcsán

A védett helyiséget az objektumvédelem alapvető fizikai védelmét biztosító eszközrendszerével kell ellátni, az elektronikus vagyonvédelem jelzőrendszer elemeit felhasználva. A védelem kialakítása során a több rétegű héj védelem kialakítása a cél. A védett helyiség kontextusában a védeni kívánt térrészt a legbelső részen elhelyezve, több védelmi réteggel körülvéve, a védett tér elszigetelésével alakíthatjuk ki a leg megfelelőbben. [61] [62] [63]

A kutatás szempontjából a hagyományos értelemben vett vagyonvédelem a következő három egységből épül fel:

- mechanikai és fizikai védelem
- elektronikai védelem, elektronikus jelzőrendszer
- élőerős védelem

Melyek áttekintve a következőek:

A mechanikai védelem az elsődleges eleme a fizikai biztonság megvalósításának. Ez az elem az, amely akadályt képezve elválasztja és fizikailag védi a védeni kívánt értéket. A mechanikai védelem a gyakorlatban is megvalósítja a behatoló értéktől való távoltartását. Valójában védi a védeni kívánt értéket. A fizikai védelem kialakítása a felhasznált anyagok függvényében tervezhető, amely egy belátható tervezett ideig ellenáll a behatolási cselekménynek. A támadó szempontjából a mechanikai védelmi elemek leküzdéséhez energiát kell, hogy befektessen a védelmi akadály leküzdésére, ami időt vesz igénybe, többnyire zajkeltéssel jár és nyomokat hagy.

A mechanikai védelem kialakítása kapcsán, az alapvető elvárás, hogy ne legyen könnyen kiiktatható. Annál megfelelőbb, minél jobban ellen tud állni a védelem ellen indított tevékenységnek. A leküzdéséhez szükséges idő, hosszabb legyen, mint az elektronikus jelzőrendszer észlelési és riasztási ideje, álljon ellen míg a beavatkozás megtörténik, az élőerős védelem megérkezik és/vagy beavatkozik. A mechanikai védelem kialakítása kettős célú. A védett objektumba megakadályozza az illetéktelen behatolást, valamint az értékek biztonságos tárolását teszi lehetővé. [43] [61] [64] [65] [46]

A mechanikai védelem elemeit tekintve a következőek:

- kerítések, sáncok
- falak, külső felületek
- nyílászárók, ajtók, ablakok, kapuk

- zárak, reteszek
- rácsszerkezetek, rácsok
- különböző minőségű fóliák
- speciális védett tárolók, szekrények, helyiségek
- biztonsági tasakok

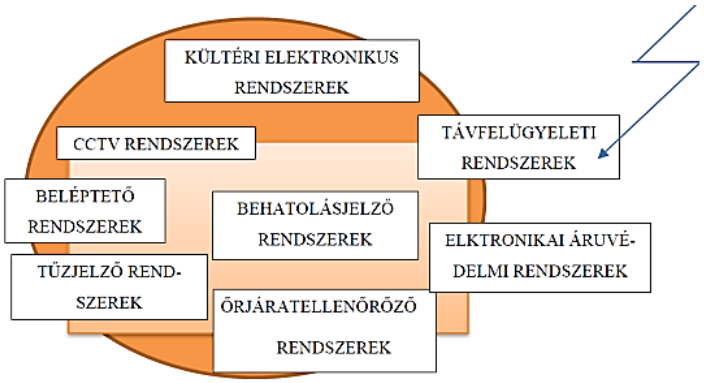
Az elektronikus vagyonvédelem a hagyományos vagyonvédelmi megoldások tekintetében tulajdonképpen az érzékelő és jelző rendszerelem funkciókat töltik be.

A védelmi struktúra kialakítása során feladat, hogy az elektronikus védelem-jelzőrendszer elemek a mechanikai védelem elemeivel kombinálva a behatolás korai szakaszában jelzést adjanak a behatolási szándék tényéről. Megfelelő kiépítés esetén az eszközrendszer zavaró jelzést legyen képes kiadni, növelve a mechanikai védelem és az őrzés hatékonyságát, illetve esetlegesen visszafordítva a behatolás szándékát. [43]

Az elektronikus jelzőrendszer részei:

- Felületvédelem, amely a védett objektumrész, térrész határoló felületeit behatolás esetén jelzéssel védi;
- Területvédelem, amely egy meghatározott terület védelmét látja el;
- Tárgyvédelem, amely egy tárgyhoz köthető konkrét jelzést lát el;
- Személyvédelem, amely személyek védelmére kialakított biztonsági jelzőrendszer.

Az elektronikus vagyonvédelmi rendszer akkor megfelelő, ha a jelzései hitelesek, azaz minimális a hibás jelzések száma. A rendszernek képesnek kell lennie adatot szolgáltatnia a riasztási cselekmény felderítéséhez, amely lehet dátum, kép és hang, valamint a felületvédelem esetén a zóna adata. Az elektronikus vagyonvédelem területeit az 5. számú ábra mutatja be szemléletesen. [64] [61] [66] [67] [56]



5. ábra Az elektronikus vagyonvédelem területei Forrás: [64] 32. oldal

Az elektronikus vagyonvédelem alkotóelemeit áttekintve a 2. számú táblázatban igen széles repertoárt sorolhatunk fel, amely elemeket végigtekintve megtalálhatóak a felületvédelem, a térvédelem és a jelzőrendszer elemei, kiegészítve a személyvédelem eszközeivel.

Objektumvédelem érzékelők	**Személyvédelem jelzők**	**Jelző készülékek**
• nyitás érzékelők • elmozdulás jelzők • ingás érzékelők • szálfeszítéses érzékelők • kontakt szőnyegek • riasztó tapéta • rácsvédő huzalozás • fóliás védelem • súlyérzékelők • hőérzékelők • nedvességérzékelők • fénysorompó • infrasorompó • passzív infra érzékelő • ultrahang érzékelő • mikrohullámú doppler érzékelő • testhang érzékelő • kapacitív érzékelő • induktív érzékelő • üvegtörés érzékelő • kombinált érzékelők • infra és mikrohullámú sorompó • videó kamera rendszer • video felügyeleti rendszer • lépésérzékelő • kerítésvédelmi eszközök	• támadásjelző nyomógomb • pénzvédő elektronika • lábkapcsoló • riasztó táska	• kül-beltéri hang jelző • átjelzők • automata telefonhívó

2. számú táblázat Az elektronikus vagyonvédelem elemei Forrás: saját ábra [44] [66] [67] alapján

A kutatás szempontjából a feldolgozás során az elektronikus vagyonvédelmi rendszer áruvédelmi és tűzvédelmi rendszer elemeinek felhasználásának vizsgálatától eltekintek. **Az élőerős védelem** az objektumvédelem kialakítása során, egységet alkot a mechanikai és elektronikus védelmi berendezések és beléptető rendszer kialakított komplex rendszerével. Az élőerős védelem a védelmi szolgáltatást megrendelő érdekeit erősíti, az objektumvédelem, vagyontárgy őrzés, személy védelem és rendezvény biztosítás kapcsán. Az élőerős védelem feladatai közé tartozik a beléptetés, a fizikai és elektronikus védelem kiegészítéseként járőrözési feladatok ellátása, valamint jogellenes

cselekmény vagy katasztrófa észlelése esetén a gyors beavatkozás. [68]

A védett helyiségek elsődleges kialakítása kapcsán, alapvető elvárás, hogy a védett helyiség a speciális, a kutatási témában később specializált információvédelmi megoldásaitól függetlenül, lehetőség szerint állami szereplő esetén feleljen meg a 90/2010. (III.26.) kormányrendelet „V. fejezet fizikai biztonság előírásainak" illetve civil alkalmazás esetén a Magyar Biztosítók Szövetsége (MABISZ) által kiadott „Betöréses lopás- és rablásbiztosítás technikai feltételei (ajánlás) 2012 március 22." kiadott ajánlásában a „4. vagyoncsoport" „A. védelmi osztályának". Teljes körű mechanikai - fizikai védelmi kialakításoknak, valamint teljes körű elektronikai jelzőrendszert kialakítva. [36] [69]

A védett helyiségnek teljes körű felület és térvédelemmel kell rendelkeznie, valamint a védett helyiségen belül ki kell alakítani a teljes körű tárgyvédelem, valamint esetlegesen a személyvédelem rendszerét is.

A védett helyiség kapcsán kialakítani kívánt vagyonvédelmi rendszernek 7/24 órás üzemben rendelkeznie kell szabotázsvédelemmel, az éles jelzéstől elkülönülő szabotázsjelzési üzemmóddal. [70]

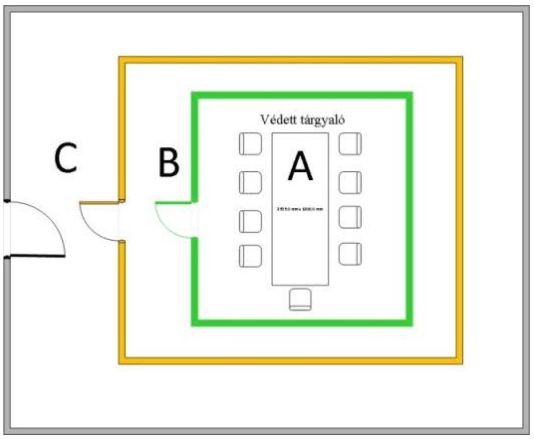
3.3 A védett helyiség épületen belüli elhelyezése

A védett helyiségek objektumon belüli elhelyezését vizsgálva egy védett helyiség kialakításának a biztonságszervezése védelmi erőforrások igénybevétele nélkül nem képzelhető el. [61] Az erőforrások növelésével a védelmi szint mértéke természetesen növelhető. A védelmi szint eléréséhez, meg kell határozni azt az arányt, ami a védeni kívánt információ értékét, és a védelem kialakításával és fenntartásával járó költségeket szembeállítja. Abban az esetben, ha megállapítást nyer a védelem kialakításának relevanciája, a II. fejezet 2.3. alfejezetében tárgyaltak alapján, akkor a következő elgondolások támpontot nyújthatnak egy a szóban forgó helyiség kialakításához. A vagyonvédelmi erőforrások típusuk alapján lehetnek technikai védelmi eszközök és élőerős megoldások. A technikai úton megvalósított védelem egyik alapeleme a mechanikai védelem. Az előzőekben tárgyaltak alapján mechanikai védelemnek tekinthető, minden olyan eszköz és technológia, valamint gépészeti és építészeti megoldás, amely a vagyon létezését vagy működését veszéllyel fenyegető szándékos ellenérdekű, jogellenes cselekményt késleltet vagy megakadályoz. A mechanikai védelem első lépcsője a kültéri védelem kialakítása, amely egy épület, vagy

épületkomplexum elhelyezéséül szolgáló terület határát jelöli ki, pontosan meghatározva azt a vonalat, amely idegen által megközelítve még nem von maga után védelmi intézkedést. Továbbá a védelem kialakításának szempontjából az a határterület, ahonnan kezdve az arányosság mértékével ki kell alakítani olyan megoldásokat, amelyek a védeni kívánt objektum, épület-biztonságát szolgálják. A kültéri védelem elemei általában kerítések, kapuk, ritkábban árkok és sáncok, azonban nagyvárosi környezetben gyakran előfordul, hogy az épülethatároló homlokzati falazat a kültéri mechanikus védelem elsődleges eleme és egyúttal a védeni kívánt objektum maga. A folyamatos üzemű objektumok védelme napjainkban elképzelhetetlen élőerős védelem működése nélkül. A külső határt kijelölő eszközrendszer megteremtésével, fel kell állítani egy őrszolgálati egységet, aminek alapfeladata a kijelölt terület rendjének a szemmel tartása, valamint az incidensek észlelése és kezelése. Az élőerős védelemnek több főből kell állnia, amely a védeni kívánt objektum méreteivel, a védeni kívánt értékek nagyságával és a belépési pontok számával arányosan kell, hogy növekedjen. Az élőerős őrzés munkáját segítik a videó kamerás megfigyelő rendszerek, amelyek megfelelő telepítés esetén a teljes objektum területét átláthatóvá teszik. [64] [61] [70] [71] A kültéri objektumvédelem megalkotása során, használatosak különböző elektronikus vagyonvédelmi rendszerek is, amelyek kimondottan külső mozgás és átlépés távérzékelésének megvalósítására lettek kifejlesztve. A megfigyelő és jelző eszközök kombinációja révén fokozható a külső tér behatolókkal szembeni védelmi hatékonysága. Egy a védett helyiség kialakítása szempontjából fontos intézkedés, hogy a védeni kívánt helyiség elhelyezését magába foglaló épületet, ellenőrizetlen formában ne közelíthesse meg senki. Az élőerős objektumvédelem feladata összetett módon, nem csak a külső részek ellenőrzése, hanem a belső épületrészek folyamatos felügyelete is, mivel komplex módon át kell látni a teljes védeni kívánt területet. A téma szempontjából elhelyezni kívánt épületrész esetén, egy speciális elhelyezési és vagyonvédelmi szemlélet követelményét kell kialakítani. A védett tárgyaló védelmi intézkedései az objektumvédelemben alkalmazott eljárás szerint héj-modellben kell, hogy kialakításra kerüljenek. Majd ezt követően alakítható ki a védelmi intézkedések specializált rendszere.

Az általános objektumvédelmi erőknek teljes körüljárhatóságot kell biztosítani a védeni kívánt helyiség külső határoló falai körül, mind horizontális, mind vertikális irányban, azonban már az őrszolgálat számára is meg kell akadályozni a középpontban álló védett tér közvetlen falazata mellé jutását. Véleményem szerint a védett helyiség térrésze körül

külön szeparált zónákat kell kialakítani, melyet a 6. számú ábrán „A, B, C" betűkkel szemléltetek.



6. ábra A védett tárgyaló elvi kialakításának alapmodellje
Forrás: saját szerkesztés

A több zónára bontott biztonsági területeket, eltérő belépési jogosultságok mellett szükséges definiálni. Az „A" zóna a védett helyiség (Komplex Védett Tárgyaló - KVT), a „B" zóna egy köztes védett tér, valamint a „C" zóna a védett helyiséget, esetünkben a védett tárgyalót körülvevő befoglaló épületrész. A speciális környezet az elképzelésem alapján az „A" és „B" zónák határoló falazata. Véleményem szerint az általános objektum őrség csak a külső „C" jelű zónát közelítheti meg. A „C" zóna területén teljes területet lefedő videó rögzítővel ellátott, és elektronikus vagyonvédelmi jelzőrendszer eszközeivel biztosítható, külön riasztási zónaként kezelhető, védelmi réteget kell kialakítani. Az átlépési pontokat a jogosultságok meghatározása mellett beléptető rendszerrel kell biztosítani. Az „A" térrész egy különleges terület, amelyre csak a „B" térrész szakaszon át vezető nyílászárókon keresztül lehet bejutni a „C" zóna felől. Az „A" térrészbe csak a védett kommunikációra (tárgyalásra) érkező személyek léphetnek be, a „C" és „B" zónák ajtó nyílásain keresztül, különleges beléptetési protokoll elvégzését követően.

Az „A, B, C" részekre csak olyan, a védett tárgyaló üzemeltetését ellátó személyek léphetnek be, akik munkájuk során a védett tárgyaló sértetlenségéért felelnek, az időszakos ellenőrzést és karbantartást végzik, vagy a védett helyiségben tartott rendezvényt biztosítják. Az általános objektumvédelem tagjai csak biztonsági incidens alkalmával közelíthetik meg azt.

3.4 A védett helyiség kialakítása

Objektumvédelmi szempontból a védett helyiségnek olyan ellenőrzött objektumrésznek kell lennie, amely folyamatos üzemű védelemmel rendelkezik és a karbantartási időszakon kívül bármikor használható szenzitív megbeszélések lefolytatására (1.3.1 alapján).

A téma tárgyául választott speciális helyiség kivitelezését, mint minden különleges építmény megvalósítását, az elhelyezés pontos megjelölésével kell kezdeni a különleges későbbi igények szem előtt tartásával. Ezek az V. fejezetben kerülnek részletes kifejtésre. A védett helyiség kialakított helyszínének, elvi és fizikai megvalósítási kritériumoknak kell, hogy megfeleljen. Elvi igény, hogy olyan épületrészt kell keresnünk, ahol a felhasználni kívánt terület felett a használónak, teljes körű jogosultsága van, és rendelkezik állandó 24 órás teljes körű bejárás lehetőségével. Biztosítottnak kell, hogy legyen a körüljárhatóság, a szemrevételezés, a műszeres vizsgálat, a karbantarthatóság. Az ellenőrzés lehetősége bármely időpillanatban szavatolt formában megvalósítható legyen. Megállapításom szerint az olyan terület amely: - csak részben körüljárható,

- közterülettel határolt, - idegen tulajdonú szomszéd épülettel közös fallal rendelkezik, - nem megoldható a teljes fizikai körüljárása és az ellenőrizhetőség követelménye,

- idegen személy által bármikor elérhető, a körülhatároló falazat akár csak egy része is, az a térrész véleményem szerint nem alkalmas a tárgybeli létesítmény megvalósítására.

A védett helyiség kialakíthatóságával kapcsolatban fizikai igény az olyan méret és kiterjedés, amely lehetővé teszi a kialakítani kívánt helyiség megfelelő számú befogadóképességét, valamint a járulékos védelmi infrastruktúra kialakításának igényeit is kielégíti.

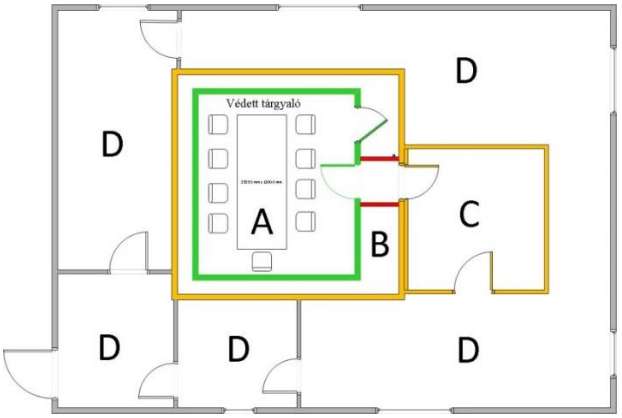
Olyan héjmodell szerkezetű helyiség megvalósítása a cél, amely mind a védelmi infrastruktúráját tekintve, mind építészeti kialakítását megteremtve (doboz a dobozban) többlépcsős védelmi modellt alkot. Ez fizikailag és építészetileg azt jelenti, hogy a befogadó helyiség határoló falai, valamint födémje és padozata nagyobb kiterjedést igényel, mint a megvalósítani kívánt védett tér mérete. Olyan környezetet kell keresnünk vagy terveznünk, ahol belső, épületrészekkel körülhatárolva tudjuk elhelyezni a védeni kívánt helyiségünket, vagy föld alatt elhelyezett szobát tudunk kiépíteni a kívánalmaknak megfelelően.

Elképzelésem szerint csak az ilyen elhelyezésű térrészben lehet a téma szempontjából

megfelelő biztonságos területet kialakítani. Egyéb megoldások esetén a maradvány kockázat mértéke jelenősen nem csökkenthető. A védett helyiségek kialakítása során az alkalmazható elektronikus vagyonvédelmi eszközök rendszerét tekintve egy ellentmondás vetődik fel, mivel egyfelől egy védett helyiséget mindenképpen el kell látni elektronikus vagyonvédelmi jelző rendszerrel, azonban másfelől véleményem szerint egy védett tárgyaló helyiségben korlátozni kell az alkalmazott elektronikus berendezések számát. Amennyiben mód van rá, el kell kerülni azok helyiségen belüli alkalmazását. Ez ellentmondást vet fel, azonban elképzelésem szerint a következőképen megvalósítható.

Amennyiben a fent említett dupla héjszerkezettel rendelkező védett terület külső körülhatároló falainak határáig az objektumvédelmi rendszer behatolás elleni védelme kialakítottnak tekinthető, akkor eljutunk addig a szintig, hogy biztosítanunk kell a 6. számú és 7. számú ábrákon köztes „B" és belső „A", a védett kommunikáció lebonyolítására létrehozott területek állandó felügyeletét és érintetlenségét.

Amennyiben a védett helyiség önállóan, egy épület középső falakkal határolt részén helyezkedik el, úgy biztosíthatóvá válik a befoglaló falak, a padozat és a mennyezet épségének felügyelete. Véleményem szerint a belső védeni kívánt területek védelmi rendszereit a védett helyiségünk környezetében, az átfogó objektumvédelemtől elkülönítve, csak a tárgyaló kezelőszemélyzete által elérhető zónába javasolt telepíteni, egyirányú átjelzés lehetőségével a központi objektumvédelem irányába. Egy megvalósítási elképzelést szemléltet a 7. számú ábra, ahol egy helyiséggel növekedett a szükséges helyiségek száma, melyet az objektumvédelmi terminológiából véve adminisztratív „C" zónának nevezek el. Az új védett térrész bevezetése esetén, szabadtér biztosítható az autonóm vagyonvédelmi felügyeleti rendszer, valamint a személybeléptetés kialakítására.



7. ábra Egy védett tárgyaló lehetséges gyakorlati kialakítása Forrás: saját szerkesztés

A 7. számú ábrán látható modell „A, B, C" részeit el kell látnunk elektronikus vagyonvédelmi jelzőrendszer elemekkel úgy, hogy a „C" és „B" részek körülhatároló szerkezeti elemei „D" irányból érkező megbontás ellen védve legyenek. A vagyonvédelmi eszközök csak a „B" és „C" határoló falazaton a külső „D" épületrészek felé néző falazaton lehetnek elhelyezve. Az „A" jelű tárgyaló falazata a falazat hordozó anyagán kívül semmilyen más anyagot, érzékelőt ne tartalmazzon, se rászerelve, se átfúrva, se beleépítve. A vagyonvédelmi elemeknek természetesen teljes körülzárást kell biztosítaniuk, így nem elhanyagolandó az épületrész alsó és felső födém szerkezetének vagyonvédelmi eszközökkel való ellátása a védett tér kialakítása során. Ez meglehetősen szigorú feltétel rendszernek látszik, azonban így szavatolható a tárgyaló külső irányból való sérthetetlenségének biztosítása.

A 7. számú ábra „B" és „C" részek falazatának „D" irányból érkező megbontás, megfúrás tényének detektálása céljából, jelzőrendszert kiépítése javasolt. Megoldás lehet a vezető szálakkal szőtt háló, amely megbontást detektáló elem. A fal szerkezetébe integrálva a vezető szál szakadása révén biztosíthatja a fal megbontása estén a jelzés generálását. Másik érzékelő megoldás az akusztikus fúrás érzékelő, amely a falban a fúró által keltett hang hatására indít riasztást.

Azon túl, hogy a védett helyiség üzemeltetésével foglakozó személyek bármely időpillanatban fizikailag ellenőrizhetik a védett helyiség teljes körülhatároló falazatát, a köztes „B" jelölésű fal külső és belső oldalán, 24 órás rögzítővel ellátott videó megfigyelőrendszerrel javasolt biztosítani az állandó felügyeletet a teljes objektumvédelmi rendszeréhez hasonlóan.

A videokamerás megfigyelőrendszert oly módon kell, kialakítani, hogy a védett helyiség és a külső részek köztes falazatának terét is figyelje, és ott esemény hatására riasztást generáljon. Továbbá a biztonság fokozása érdekében, egy az előzőektől független elektronikus riasztórendszert szükséges kialakítani az elektronikus vagyonvédelemben szokásos érzékelő elemek felhasználásával, önálló védett zónát - zónákat létrehozva.

A fizikai védelem kialakításának további speciális eleme a nyílászáró, amely a védett tárgyaló előterébe, és a tárgyalóba enged bebocsájtást. Az ajtóknak mechanikailag és információbiztonságilag is egységes egyenszilárdságú felületet kell, hogy alkossanak a határoló falakkal. Mind fizikai behatolás ellen kell, hogy ellenálljanak, mind a későbbi fejezetben indokot okok miatt rádiósan és akusztikusan kell, hogy csillapítsanak. Az egyéni vagyonvédelmi rendszer számára állapotjelet kell, hogy szolgáltassanak a nyitott és zárt állapotukat illetően. A 7. számú ábra „C" helyiségébe „D" irányából történő

belépésre olyan nyílászáró beépítése lehet a követelmény, amely viszonylag nagy átjutási idővel rendelkezik és megtalálható rajta minden olyan elem, amely jelzi az átjutás kísérletét vagy tényét. Továbbá mint egyetlen belépési pont a védett tér irányába, követelmény egy beléptető rendszer kialakítása is, amely rendszer a belépési jogosultságok pontos meghatározása mellett regisztrálja az áthaladó forgalmat. Elképzelhető a kialakítástól függően bármilyen elvű beléptető megoldás, a tudás alapú rendszerektől kezdve a birtok alapú rendszereken át a korszerű biometrikus rendszerek felhasználásáig. A 7. számú ábra „C" helyiségéből „A" helyiségébe vezető nyílászárója úgy képzelhető el, hogy két olyan ajtó kerül egymás mögé beépítésre, amelyek egymást nem akadályozzák a működésben és a funkciókat elosztva teljesítik az előírt fizikai és mechanikus kívánalmakat (V. fejezetben kerül részletezésre). A védett helyiség kialakítása során a menekülési útvonalat megfelelő módon jelölni kell.

A leírt megközelítések alapján a védeni kívánt helyiség közvetlen külső környezete csak regisztrált és rögzített módon közelíthető meg, és a határoló felületeit érő behatások naplózást generáló eseményt idéznek elő. A védett helyiség információbiztonságának megteremtése érdekében egyéni személyi beléptetés kialakítását tartom indokoltnak. Az átvizsgálás kiterjed a csomagröntgen alkalmazására, valamint a személyi beléptetések során alkalmazott kapuk használatára, illetve a napjainkban elterjedő testszkenner alkalmazására. A testszkennerek meglehetősen érzékenyek, valamint elég felbontással rendelkeznek az esetlegesen ruházatban rejtőző, fenyegetést jelentő tárgyak vagy technológiák felderítésére. A kialakítások technikai értékeire az V. fejezetben teszek javaslatot.

ÖSSZEGZÉS

Jelen fejezetben a harmadik hipotézis megválaszolása során, tovább szűkítem a védett helyiség kialakításának kutatási irányvonalát. Az információbiztonság elméleti PPT modelljét felhasználva szemléltetem a kutatás szempontjából releváns irányvonalat, amely a fizikai kialakítást és a védett helyiség elhelyezését helyezi fókuszába. A téma feldolgozása során áttekintem az objektumvédelem technikai összetevőit. Elképzelésem alapján egy védett helyiség elsődleges megközelítés alapján, meg kell, hogy feleljen egy kiemelten őrzött fizikai környezetnek. A védeni kívánt térrész a hagyományosnak tekinthető objektumvédelmi megoldások révén kerül kialakításra a fizikai védelem az elektronikus védelem és az élőerős védelem felhasználásával, a besorolt állami és magánszektorban megvalósítható szerkezetet alkotva. Az objektumvédelem összetevőinek áttekintését követően ajánlást teszek egy védett helyiség objektumon belüli elhelyezésének lehetséges módjára, és az autonóm védelmi infrastruktúra kialakítására. Továbbá javaslatot teszek olyan védett helyiség struktúrára, amely a besorolt állami és magánszektorban megvalósítható.

IV. FENYEGETETTSÉGEK FELTÁRÁSA, CSOPORTOSÍTÁSA

A fejezet célja a negyedik és ötödik hipotézispontom vizsgálata. Csoportosítom a védett helyiségek kapcsán felmerülő, az információbiztonság állapotát veszélyeztető, az általános egyéni eszközös technikai hírszerzés módszereit összegző tevékenységeket. Csoportosítom a védett helyiségek információbiztonságára fenyegetést jelentő technikai eszközöket, amely alapja a védett helyiség kialakításához szükséges védelmi módszerek megállapításának. Feldolgozom és a gyakorlatban igazolom az ember-ember közötti közvetlen kommunikáció során megjelenő információbiztonsági kockázatokat hordozó jelenségeket. Áttekintem az offenzív technikai eszközök piaci helyzetét. Konkretizálom a védett helyiség kialakítása kapcsán feltételezhető támadási lehetőségeket.

BEVEZETÉS

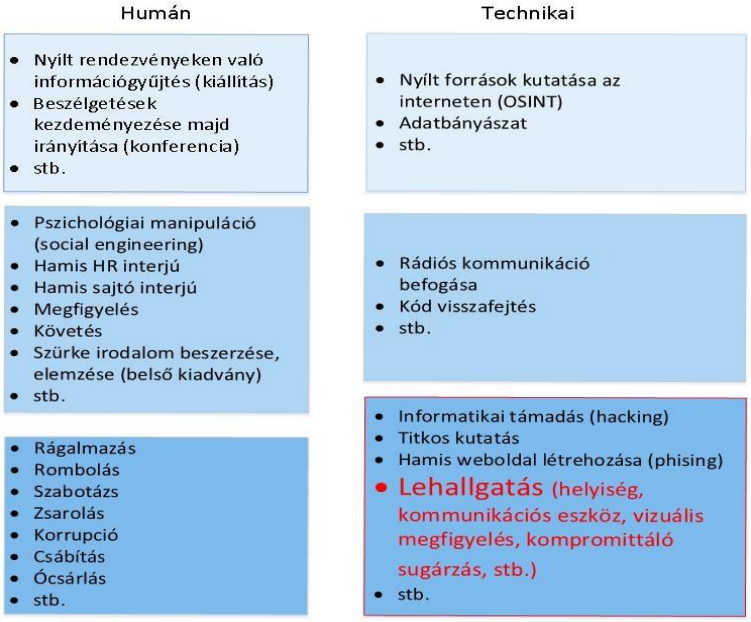
Az információszerzés módszereit áttekintve megjelölöm a kutatás további irányát. Ezt követően áttekintem a hírközlés elméleti modelljét a téma szempontjához illesztve. Majd az ember-ember közötti kommunikáció során létrejövő csatornákat sorra veszem és először megvizsgálom és kísérlettel igazolom a helyiségben elhangzott kommunikáció tartalom információbiztonsági aggályait. A továbbiakban áttekintem és kísérlettel igazolom a helyiségekben megjelenő vizuális tartalmak megjelenésével kapcsolatos információbiztonsági problémát. Ezt követően áttekintem a digitális megjelenítők alkalmazása kapcsán felmerülő kompromittáló elektromágneses sugárzások által hordozott információbiztonsági problémát, és kísérletsorozattal igazolom a probléma fennállását.

Az egyéni technikai eszközökkel történő hírszerzés módszerei tekintetében a kutatás során számos módszer elvi lehetősége merült fel, melyek összegzése átfogó képet nyújt a lehetséges információszerzési módokról. A technikai hírszerzés módjait összefoglalva, az információbiztonsági kockázatok felvetését igazolva, valamint a védeni kívánt helyiségek támadási vektorait vizsgálva, feltárom a kutatás fókusza szempontjából lényeges, az információbiztonság állapotát fenyegető műszaki megoldások lehetőségeit. A kutatás ezen részében összefoglalva beazonosítom a közvetlen humán kommunikáció folyamán létrejövő, az információbiztonságot közvetlenül veszélyeztető elektronikus támadóeszközök fő jellemzőit, a szakirodalmi kutatás és a nyílt médiatartalmakban fellelhető források felhasználásával. A témában internetes keresést végeztem, amely alapján megállapítottam az egyéni technikai hírszerző eszközök jelentős szabadpiaci

elérésének tényét. A kutatási szakasz eredményeként osztályozom a témában releváns megfigyelésre alkalmas berendezések alapparamétereit, kiemelve azon paramétereket, amelyek kiiktatásával – kiküszöbölésével, az adott fenyegetettség megszüntethető, vagy az alkalmazhatósága válik nagymértékben nehézkessé, jelentős többlet terhet okozva a támadó jellegű kialakítás szempontjából. A kutatás részeként foglalkozom a trendet követő SMART folyamatokkal, valamint a védett helyiség és SMART folyamat ellentmondásával. Az IT eszközök alkalmazása jelentős információbiztonsági kockázatot jelenthet egy védett helyiség üzeme kapcsán. Érintőlegesen kitérek a jelentősebb kibertámadások jelenlegi statisztikájára, szemléltetve az IT eszközök által hordozott információbiztonsági kockázatok problémáját.

4.1 Az információszerzés elemei

Az információszerzés célját tekintve egy komplex mechanizmus. A megvalósítás kimeneti outputja, jelen kutatás első fejezetének részletes tudományos okfejtéséből kiindulva, minden esetben az információt megszerezni kívánó egyén, vagy szervezet előnyökhöz való jutása. A lehetőségeket tanulmányozva az információszerzés eszköztárának széles vertikumát találjuk, a támadó lehetőségek kapcsán. A módszereket - eszközöket nagyrészt halmazokba csoportosíthatjuk, de valójában két nagy halmazról beszélhetünk, amely az alábbi 8. számú ábrán kerül bemutatásra.



8. ábra Az információszerzés módjai Forrás: [72] 345. oldal alapján, saját szerkesztés

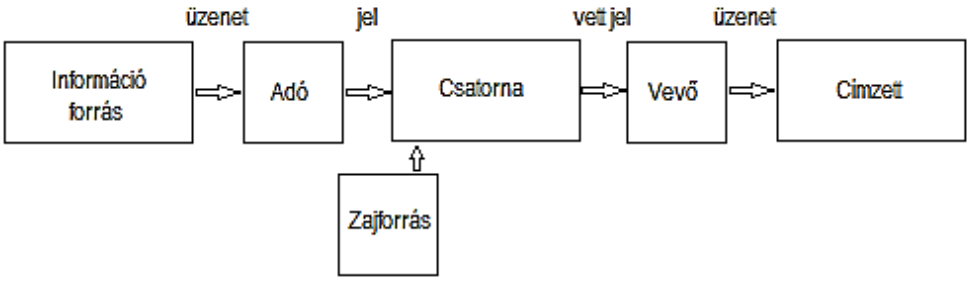
A két oszlop halmazelemeit áttekintve az információszerzés lehetőségeinek volumene a

humán és technikai jellegű módszerek csoportjaira bontható. A humán oszlop elemeinek lényege, hogy az embert, mint adat, - és információ hordozót felhasználva, az egyéni viselkedési és kommunikációs megnyilvánulásokat figyelve-befolyásolva, részben pszichológiai elemeket felhasználva éri el az információszerzés célját. Az ábra másik oszlopa az információszerzés technikai jellegű elvi módszereinek összegzését mutatja be, amely elemeinek áttekintése során konkrétan behatárolható a kutatási téma elsődleges, - a védett helyiségek információbiztonsága szempontjából fenyegetést jelentő technikai információszerzési lehetőség - iránya, a lehallgatás. Ebben az esetben az információk bizalmasságára az audiovizuális kommunikáció útján megjelenő, információt hordozó fizikai jelenségek valamilyen, a technika által kínált megoldás útján megvalósítható érzékelése, megszerzése jelenti a fenyegetettséget. [73]

Az értekezés előző részeiben tárgyaltak alapján látható, hogy az információszerzés elemei széles skálán mozognak, külön kutatási irányokat teremtve a témakörben, amelyek további önálló kutatási téma alapjául is szolgálhatnak. Ki kell jelentenem, hogy a „Humán" és IT rendszereken történő információszerzés lehetőségeinek vizsgálata nem jelen kutatás témája, azonban a teljesség kedvéért a védett helyiségek komplex biztonsága kutatási terület irányának további behatárolásához szükséges azokat megjeleníteni. Az IT rendszerek védett helyiségekben történő alkalmazása nem kívánatos, azonban a SMART-osodási folyamatok eredményeként problémát okoznak. A fenyegetettségek feldolgozása során jelen fejezetben a kutatás részeként a későbbiekben tárgyalásra kerül. [74] [47]

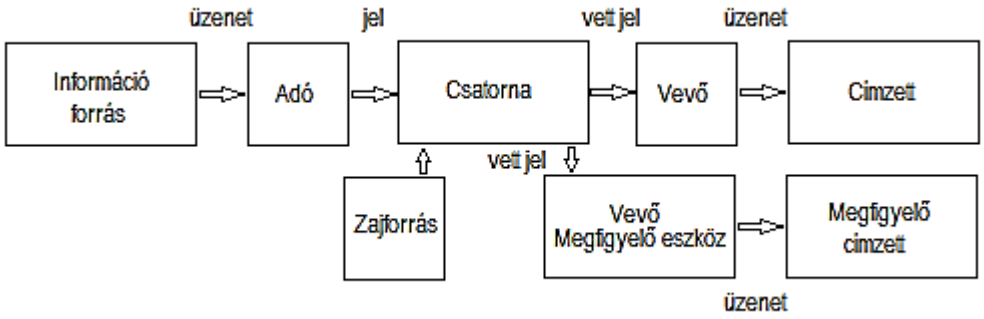
A 8. ábra technikai elemek oszlop a lehallgatás halmazelemének kutatása, döntően befolyásolja a védett helyiség kialakításának műszaki paramétereit. Közvetlenül és szorosan kapcsolódik a célként megalkotni kívánt környezet kialakításához.

Az ember-ember közvetlen kommunikáció környezetének lehallgatása szempontjából, a tudományos elméleti hátteret tanulmányozva, a Shannon - Weaver féle hírközlési modellt kell tanulmányozni amelyen keresztül szemléletesen bemutatható a folyamat. [75] [76] A 9. számú ábrán megjelenített kommunikációs folyamat szemlélteti az információ átvitel összetevőit. A kommunikáció alkalmával a védett közegből történő kilépés során az információforrást és az adót kell elsőként figyelembe venni a kutatás szempontjából. Ezek az I. fejezet 2. ábrája alapján az emberi hang, a rezgés, a megjelenítő eszközről verődő vagy kibocsájtott fény nyalábja, valamint elektronikus készülék esetén, nem tervezett információt hordozó elektromágneses jel sugárzása.



9. ábra Shannon - Weaver féle hírközlési modell Forrás: [77] alapján [22] [78]

Az ember-ember közvetlen kommunikáció során az átviteli csatorna a kommunikációt körülvevő térrész anyaga, amely elsődlegesen a térrészt kitöltő levegő közege, másodlagos csatornaként a megjelenő fizikai jelenségekkel kölcsönhatásba lépő anyagok közege, amelyek fizikai jeltovábbító csatornákat hoznak létre. A vevő és a címzettek a kommunikációt fogadó fél érzékszervei, valamint a felismerés tudata, amely dekódolja az információforrás és adó által kibocsájtott, a csatornán keresztül érkező információt. A kommunikáció csatornáihoz természetesen, mint minden átvitelhez, zaj is keveredik, amely mértéke meghatározza a kommunikáció minőségét és érthetőségét. [79] Az elvi modell alapján a technikai lehallgatás elméleti megvalósítása a csatorna jellemzőinek megfigyelését jelenti, amely módosított hírközlési modellje a 10. számú ábrán látható. Ha az átviteli csatorna fizikai jellemzői megfigyelő eszközzel detektálhatóak, és a hasznos jel és zaj viszonya nem lépi túl az értelmezhetőség határát, akkor a vevő megfigyelő eszközre jellemző érzékelési paraméter szerint a csatorna információtartalma megfigyelhetővé válik. Ennek folyamata a csatornából kicsatolt megfigyelő eszközbe tovább menő vett jel - vevő megfigyelő eszköz - üzenet - megfigyelő címzett út.



10. ábra Módosított Shannon - Weaver féle hírközlési modell Forrás: saját szerkesztés

A védett helyiségek szempontjából a módosított hírközlési modell - vevő megfigyelő eszköz- révén kialakult csatornáját kell ellehetetleníteni, amely az értelmezhetőség jel-zaj viszonyának teljes elrontásával, vagy a hírközlési modell teljesen zárttá tételével valósítható meg. Az első lehetőség során a - vett jel - vevő megfigyelő vevő- úton a jelben lévő érzékelhető zaj mértékének növelése révén zárható ki a - vevő megfigyelő eszköz- által vett üzenet értelmezhetősége. Míg a második lehetőség esetén, a vevő megfigyelő eszköz csatornához való hozzáférését kell kizárni, ellehetetlenítve a folyamatot. Zárt rendszert alkotva a modell átviteli útját zárt módon kialakítva, az információforrás és a címzett közötti közeget hermetikusan elzárva, ellehetetleníthető a kicsatolási folyamat.

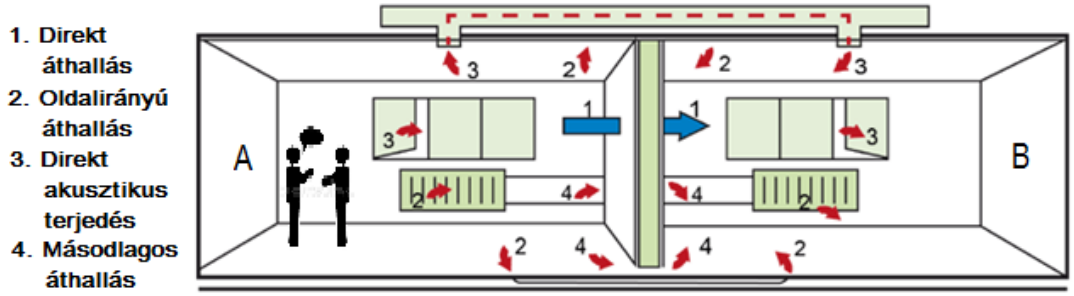
4.1.1 A védett helyiségekben megjelenő audio tartalom információbiztonsági problémái

A biztonsági rést jelentő fizikai jelenségek közül, elsőként a hang útján terjedő és ezzel együtt az információ akusztikus fizikai terjedését okozó jelenségeket kell megvizsgálni. Egy helyiségben létrejövő ember-ember közötti kommunikáció során elsősorban az emberi hang az elsődleges kommunikációs forma. Az információ tartalmú gondolat a beszéd biológiai mechanizmusainak során a beszélő hangszálain megjelenik, melyek ott mechanikai rezgéseket keltenek. A keletkező mechanikus rezgések, a beszédképzés folyamatai során a beszéd erősségétől függően, a hangszálak felülete által hullámokat hoznak létre a személyt körülvevő levegővel kitöltött környezetben, a körülvevő közeg által. [80]

Jelen esetben, mint elsődleges kommunikációs átviteli közeg, direkt módon érkezik a hallgató kommunikációs partner-partnerek halló járatába, ezzel szintén az információ tartalommal modulált rezgést létrehozva a dobhártya felületén. A hallgató kommunikációs partner, a hallás folyamata során a hallószervével érzékelt rezgéseket az agy által, a hallás biológiai folyamatán keresztül feldolgozza, és értelmezi, így létrehozva az információ fogadását. Az információ tartalmú légrezgések (léghangok) azonban természetesen nem csak a hallgató fülébe jutnak el, hanem a beszélő teljes környezetében megjelennek, a légnemű közegre jellemző terjedésnek, verődésnek és csillapításnak megfelelő erősségben. A falazatban és a környezetben lévő tárgyakban is tovaterjednek (testhang) formájában. A hang terjedési sebessége +15°C levegőben 340,8m/s, vasban 5170m/s, betonban 3400m/s, téglafal 1460-2800m/s gipszlemezben

2400m/s, mészhomok téglában 1460-2740m/s, acélban 5100m/s, üvegben 4900m/s. [81] [82]

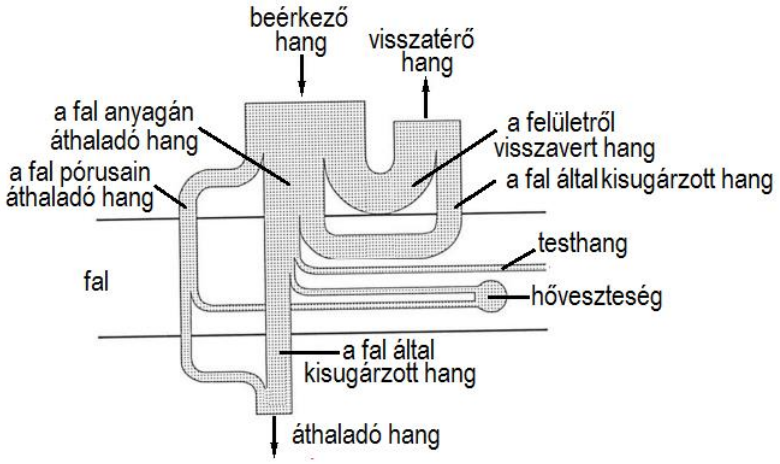
A levegőben terjedő hanghullámok ugyan a távolság növekedése révén csillapodnak, azonban a kommunikáció során, olyan erősségben jelennek meg, amelyek eljutnak a körülvevő helyiség felületeihez is, ott másodlagos és további rezgéseket létrehozva. Egy ilyen modell ábráját láthatjuk a következő 11. számú ábrán. Az ábra kettő, „A" és „B" betűkkel jelölt szobát jelenít meg.



11. ábra A hangrezgés lehetséges terjedése a szomszédos épületrészek között Forrás: [83] alapján

Amennyiben az „A" forrás helyiségben akusztikus hang keletkezik, az a levegőt megrezgetve, abban hullámokat előidézve a forrásból tovaterjed a hangforrást körülvevő térben. A hang az ember számára direkt érthető információt hordozva szétterjed, így az információ eljut a szobában lévők füléig. A hang – megfelelő ellenintézkedés hiányában – nem áll meg a helyiség határoló falainál, hanem egy része a levegőben terjedő akusztikus hullámként, egy része mechanikus rezgésként tovább terjed a szomszédos helyiségek irányába, így az információ nem kívánt helyekre is eljuthat. A szomszéd helyiségben (helyiségekben), valamint a szobán átmenő infrastruktúra elemein érzékelőket elhelyezve, a forrásszobában elhangzó akusztikus rezgés, mérhető, érzékelhető és rögzíthető lehet.

A hangok falon keresztüli átvitele több terjedési úton valósulhat meg. Az egyik a diafragma-hatás ahol falpórusokon keresztül történik az átvitel. A másik az átvezetés, amely a fal anyagán keresztül történik hosszanti és hajlítási rezgések formájában. Az átvitt hangok mind a falban, mind a szomszédos helyiségben -a téma szempontjából, információtartalommal rendelkező- rezgéseket keltenek. A hangvezetés, amely a szilárd testekben történő hangvezetés útján terjed, testhangként jelentkezik. A hang falazatnak való ütközésekor történő terjedését a következő 12. számú ábra szemlélteti.



12. ábra A falnak ütköző hangenergia megoszlása R. Berger szerint
Forrás: [82]148.oldal alapján saját készítésű ábra

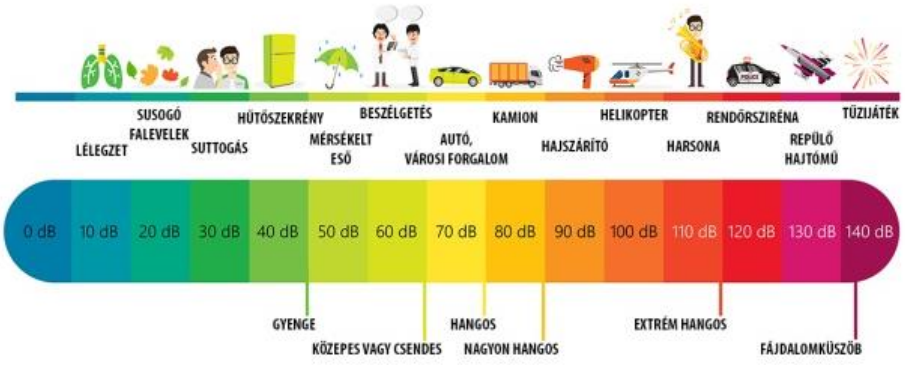
A léghangok falazaton történő átjutását két módon tudjuk megakadályozni. Az egyik, ha olyan tulajdonságú-vastagságú falazatot építünk, amelyben nem képesek hosszanti és hajlítási rezgések kialakulni. A másik, ha többrétegű falazatot készítünk légrések közbeiktatásával, melyekben a hullámok le tudnak csillapodni. A léghangok szomszédos környezetből történő detektálására kísérletet végeztem, amely összefoglalóját a következő 1. számú vizsgálat tartalmazza. [82] [81] [84]

1. vizsgálat:

A hang terjedésének és helyiség környezetében kívülről történő érzékelésének bizonyítására akusztikus indikáló méréseket végeztem, amelyek értékelése révén bizonyítottá vált az elméleti feltételezés, miszerint egy épületrész hang alapú kommunikációs környezete a megjelenő fizikai jelenségek révén a szomszédos épületrészekben is érzékelhetővé válik. Ezzel bizonyítva a biztonsági rés fennállását a modell helyiségben elhangzó akusztikus információk szivárgására. Bizonyítva az információ tartalmú rezgések kommunikációs helyiségen kívüli érzékelehetőségét, igazolódik a védett helyiség akusztikus árnyékolásának relevanciája.

A mérés során, egy helyiségben elhelyezésre került egy hangforrás, valamint a hangforrástól 1m-re egy zajszintmérő eszköz. A hangforráson 1kHz szinuszos hang került kisugárzásra úgy, hogy a zajszintmérő 60dB értéket mutasson.

Az 60dB érték a beszéd hangjának felel meg, melyet az alábbi 13. számú ábrán tekinthetünk meg.

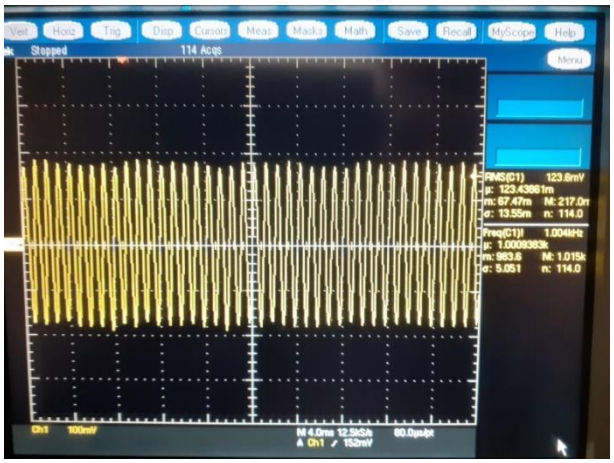


13. ábra Decibel érték a hang erejének szemléltetésére Forrás: [85]

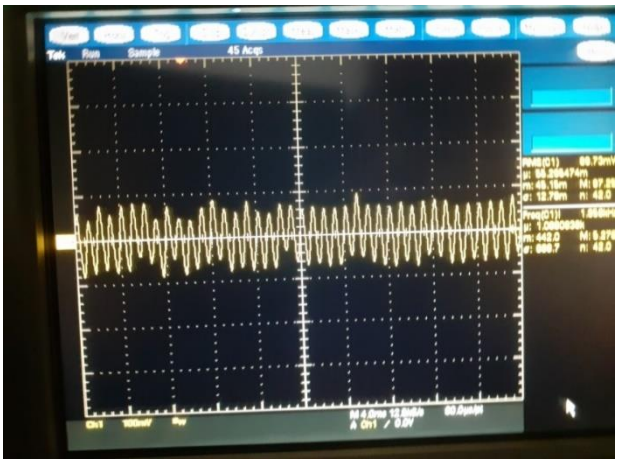
A kisugárzott hang vizsgálatára kétféle szenzort alkalmaztam. Az egyik szenzor egy erősítővel ellátott miniatűr mikrofon (hallókészülék kivezetett erősítővel), a másik szenzor pedig egy az akusztikus hangszerek hangosítása során használt, felületi hangrezgés érzékelésére használt aktív erősítős kontaktmikrofon.

A két érzékelő típus használatát a vizsgált paraméterek adták, miszerint az elsővel a levegő útján hordozott információ terjedését, míg a másodikkal pedig a rezgés típusú másodlagos terjedést demonstráltam. A mérés célja a szomszédos helyiségekben megjelenő akusztikus információ érzékelhetőségének vizsgálata abból a szempontból, hogy milyen körülmények esetén érzékelhető és indikálható a forrás helyiségben lévő hanggenerátor hangja. Az 1kHz-es hanghullám terjedését demonstrálva, bizonyítható az információbiztonsági rés. A vizualizációs szemléltetésre oszcilloszkópot használtam. Itt jegyzem meg, hogy mérés során, a falazati anyagok csillapítási értékének vizsgálata nem volt cél.

A vizsgálat során bebizonyosodott, hogy az akusztikus, légcsatolású mikrofont a forrás helyiségben bárhol elhelyezve, valamint a szomszédos helyiségben a közvetlen levegő csatolású átvezetőkben (átvezető furat a falon), átvezető csövekben (átvezető kábelcsatorna), külső ablakpárkányon nyitott ablaknál, szellőztető berendezés csöve, csendes külső környezet esetén szomszédos helyiség légtere, mindenhol értékelhető és vizualizálható eredményt adott a mérés. A forrás szinusz jel különböző amplitúdókban mindenütt elérhető volt. Az indikációs mérés vizuális oszcilloszkóp ábrái a következő 14. és 15. ábrákon láthatóak.

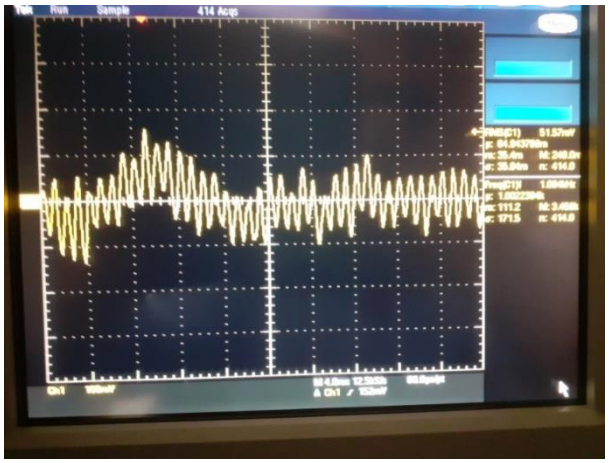


14. ábra Forrás helyiségben lévő légcsatolású mikrofon jelének képe
Forrás: saját szerkesztés

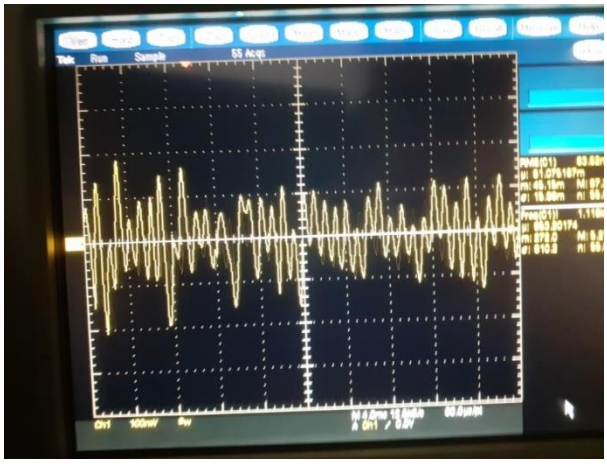


15. ábra Forráshelyiséggel légkapcsolatban lévő, falon átvezető nyílásban elhelyezett, légcsatolású mikrofon jelének képe
Forrás: Saját szerkesztés

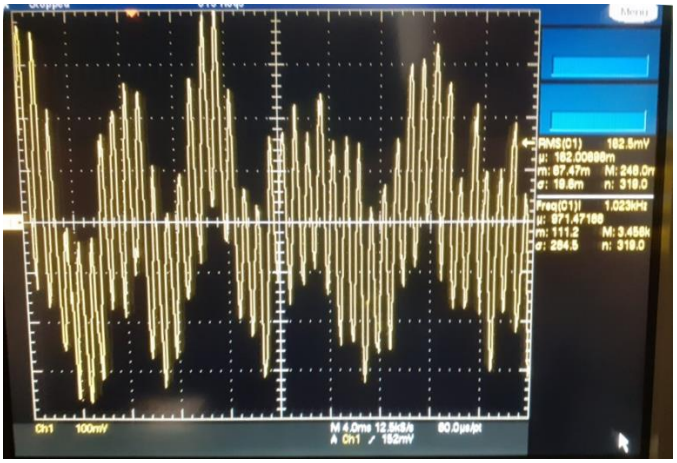
A kontakt mikrofonnal végzett mérés során a határoló falszerkezet túlnyomó részében, valamint az átvezetett épületgépészeti elemeken, nagymértékben volt kimutatható a forrás jel. A kontakt érzékelővel végzett indikációs mérés vizuális oszcilloszkóp ábrái a következő 16., 17. és 18. ábrákon láthatóak.



16. ábra Forráshelyiséggel szomszédos falazaton elhelyezett, kontakteszköz jelének képe
Forrás: saját szerkesztés



17. ábra Forráshelyiséggel szomszédos, közös gépészeti csövezéssel rendelkező fűtőtesten elhelyezett, kontakteszköz jelének képe
Forrás: saját szerkesztés



18. ábra Forráshelyiség ablak nyílászáró felületén elhelyezett, kontakteszköz jelének képe
Forrás: saját szerkesztés

A fűtőrendszer elemein történő mérés során, valamint az utcafront felőli nyílászárókon végzett kísérlettel bebizonyosodott, hogy a gépészethez használt aktív villamos motoros elemek (szivattyúk) zaja, valamint a nyílászárók külső felülete felől jövő zajok hatása, negatív értékben befolyásolják az indikálás hatásfokát (jelentős zaj keveredik az átviteli csatornába).

1. értékelés:

A vizsgálat során bebizonyosodott, hogy a védett helyiségek kialakítása kapcsán első számú fontossággal bír a kommunikáció során létrehozott, információ tartalmú, megjelenő hang védelme. A megjelenő hang hullámai nem csak a kommunikáció helyszínéül szolgáló helyiségben vannak jelen, hanem a szomszédos környezetben is. Az indikáló mérés során bebizonyosodott, hogy egyenes csatornájú hangvezetés során akár két helyiséggel távolabb is detektálható a forrás helyiségben előálló hang hulláma. Ezért védett helyiség kialakítása kapcsán bizonyítást nyert az akusztikus csillapítás, valamit körülhatárolt héjszerkezetű elszigetelés kialakításának a szükségessége a kommunikáció során keletkező, védeni kívánt hang elvi megfigyelésének teljes kizárása érdekében.

4.1.2 Védett helyiségekben megjelenő vizuális tartalom információbiztonsági problémái

A védett helyiségek kapcsán a biztonsági rést jelentő fizikai jelenségek közül másodikként a vizuális úton létrejövő, az információt fény útján közvetítő terjedését kell, hogy megvizsgáljuk. Egy helyiségben létrejövő ember-ember közötti kommunikáció során másodikként, a szavakkal történő kommunikációt követően az emberi látás a leggyakoribb kommunikációs forma. Ez esetben az információ tartalmú gondolat, cselekedet a vizualizáció útján jut el az információ forrástól a címzettig. A megjeleníteni kívánt gondolatot, - az információ forrása - az adó, az emberi közlést valamilyen megjelenítőn keresztül juttatja az átviteli csatornába. A csatorna a kommunikációs környezetet körülvevő térrész, amelyben a fény fotonja által terjed az információ c=300000km/s sebességgel. [86] A fény fotonjai, amelyek jelen esetben az információ tartalmú jelet alkotják, a kommunikációs címzett szemében jelennek meg mint vevőben. Ebben az esetben a szem, mint vevő érzékeli az értelem számára felfogható jeleket, és a látás biológiai mechanizmusán keresztül jut az információ a kommunikációs partner

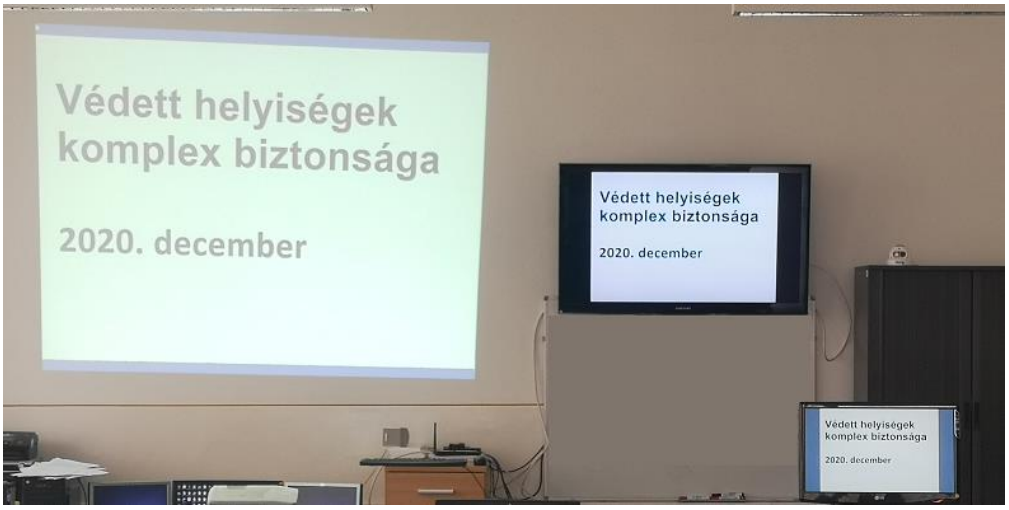
tudatába. [22] [81]

A védett helyiségek szempontjából a megjelenítendő információ átviteli csatornája a kommunikációs térrész kitöltő közege, a levegő. A vizuális tartalom védelmére irányuló kutatás során véleményem szerint nem csak az információ vizuális tartalma lehet a védeni kívánt információ, hanem a kommunikáló partnerek kiléte is, így többlet intézkedést igényelve a kialakítás során. A védett helyiségek kialakítása szempontjából, a helyiségen kívüli optikai rálátás esetén, információbiztonsági rést állapítok meg, amely feltételezést kísérlettel igazolok. A téma kontextusában további kockázatot jelentenek a közvetlen eseményeket megfigyelő, vizuális ellenőrzést lehetővé tévő eszközök is, melyek helyiségen belüli elhelyezésével megfigyelhető az ott történt esemény. Az ilyen eszközök kivédését a védett helyiségbe történő megfigyelőeszköz bejutásának megakadályozásával és a helyiség homogenitásának biztosításával érhetjük el.

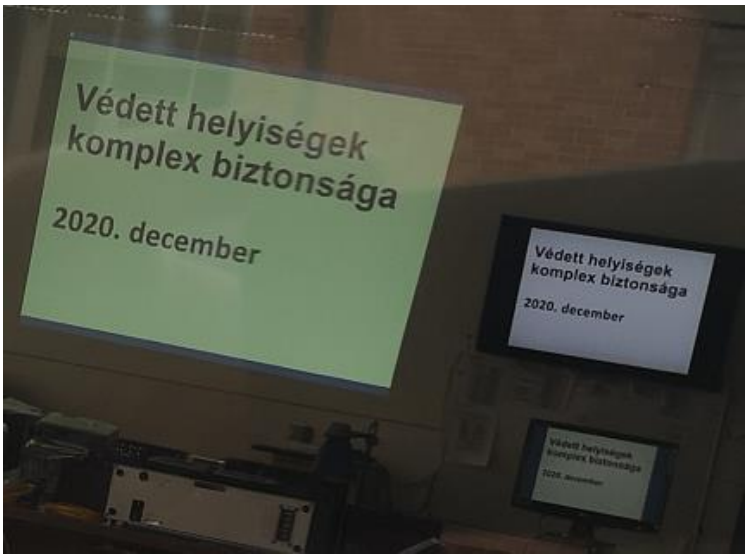
2. vizsgálat

A vizsgálat során egy triviális kísérletet végeztem, amely célja bebizonyítani, hogy optikai rálátás esetén a különböző védett helyiség kialakítások során, kerülni javasolt a külvilág felé nyitott, tiszta optikai rálátás kialakítását.

A kísérlet során három különböző méretű prezentációra alkalmas megjelenítő képét figyeltem meg, amelyek teljes rálátással rendelkeznek a külvilág felé. A kísérlet során mindenféle nehézség nélkül leolvasható volt a kivetítők tartalma. A kísérletet egyszerű mobiltelefonnal két távolságból dokumentáltam, melynek képei a következő 19., 20. és 21. számú ábrán láthatóak.



19. ábra Nyílt optikai felületekkel rendelkező kommunikációs környezet beltéri képe
Forrás: saját szerkesztés



20. ábra Nyílt optikai felületekkel rendelkező kommunikációs környezet dupla üvegen keresztül, az üveg felületéhez közel készített kísérlet képe
Forrás: saját szerkesztés

21. ábra Nyílt optikai felületekkel rendelkező kommunikációs környezet, szomszéd épületből, két ablak nyílászárón keresztül készített képe
Forrás: saját szerkesztés

2. értékelés

A vizsgálat során bebizonyosodott, hogy a védett helyiségek kialakítása kapcsán relevanciával bír a kommunikációs környezetben megjelenő, információ tartalmú vizuális elemek védelme. A megjelenő fény fotonjai nem csak a kommunikáció helyszínéül szolgáló helyiségben vannak jelen, hanem a rálátás és betekintési szögön belüli környezetben is, a láthatóság fizikai jellemzőinek korlátaival. A kísérlet során tapasztalt torzulást a modell kommunikációs környezet határoló üvegeinek torzítása, és a rögzítőként használt mobiltelefon véges számú felbontása okozta. A védett helyiség kialakítása kapcsán bizonyítást nyert a külső betekintés megakadályozásának a szükségessége, a kommunikáció során keletkező, védeni kívánt vizuális információ megfigyelésének teljes kizárása érdekében.

4.1.3 Védett helyiségekben alkalmazni kívánt vizuális megjelenítők információbiztonsági problémái

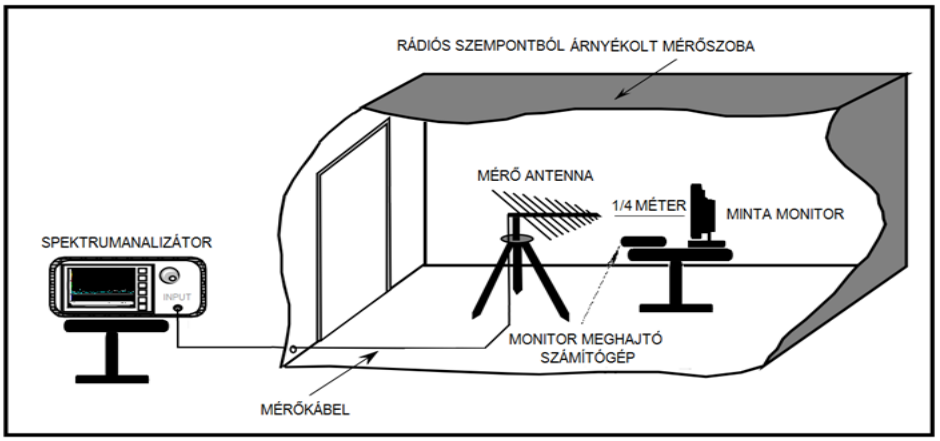
A védett helyiségek kockázati elemeinek kutatása kapcsán, jelen alfejezetben a képi megjelenítőkhöz kapcsolódó, biztonsági rést jelentő kockázati tényezőket vizsgálom, amelyek a megjelenítő eszközök működtetéséből - működéséből származó kockázatok. [87] A prezentációs technológiák megvalósítása manapság aligha elképzelhető valamilyen digitális megjelenítő nélkül. Azonban a védett helyiségek vizualizációs technikai eszközzel történő felszerelése, számos információbiztonsági problémát vet fel. A problémák több csoportra bonthatók. Az egyik csoport tisztán informatikai jellegű, amely a vizualizációs megjelenítő eszköz megbízható szoftveres üzemeltetését jelenti. A másik csoport, amely a védett helyiség kialakítása szempontjából szorosan kapcsolódik az üzemeltetett elektronikus berendezések működéséből származó információ tartalmú fizikai jelenségek vizsgálatához. A megjelenítő eszközök által keltett fizikai jelenségek egyik alapvető eleme a hangszórók által keltett, a beszéd információbiztonsági felületeivel megegyező fizikai jelenségek csoportja, amely az előzőekben tárgyalásra került. A téma második csoportja a fény útján keletkező sugárzások csoportja, amely direkt megjelenési forma, az előzőekben szintén tárgyalásra került. Azonban harmadik csoportként beszélhetünk a megjelenítő eszközök által keltett elektromágneses sugárzások megjelenéséről, amelyek egy része információ tartalommal terjed a kommunikációs tér környezetében. Az ilyen jellegű sugárzások a megjelenítő eszközök nem tervezett funkciója, többnyire a működés során előálló jelek másodlagos hatása. A probléma forrása az elektromos megjelenítő készülékekben, a rendeltetésszerű működés során létrejövő, az alkatrészek és áramköri vezetők felületéről kibocsájtott rádiós hullámok megjelenése, amelyek a készülékekben előálló váltakozó periódusú jelekből állnak elő. A védett helyiségek kialakítása szempontjából a feladatot a kisugárzott jelek helyiség határoló falazatán belül tartása adja, amelyet a védelmi intézkedés kialakítása során figyelembe kell venni. A témát kutatva és elemezve érdekes információbiztonsági és rádiótechnikai probléma körvonalazódott, miszerint lehetőség szerint bizonyítást érdemlően kell hivatkozni az információbiztonsági probléma fennállásáról. A témát kutatva, szakmai egyeztetéseket folytatva, ellentmondásos véleményekkel találkoztam, miszerint a probléma fennállásának ténye megosztó eredményt mutat. A megosztó szakmabeli vélemények hatására, célul tűztem ki a téma részletesebb vizsgálatát, és lehetőség szerint a probléma demonstrálását.

A problémakör nyílt forrásokból való kutatása során két irányt határoztam meg. Az

egyik a védelmi intézkedésekre vonatkozik „TEMPEST" néven, amely a kompromittáló elektromágneses kisugárzás elleni védelem eszközeiről szól. Ez a témakör a kutatás során hiányos hozzáféréssel áll rendelkezésre, a témával foglalkozó állami szervezet hivatalos közlése alapján a téma egyes részei nem nyilvános hozzáférésűek. [88] [24] [89] [90] A másik irány, amely jelen fejezet témája, a probléma fennállásának bizonyítása. A bizonyítás részeként számos rádiós mérést végeztem a megjelenítő interfészek rádiós kisugárzásának felderítése érdekében, továbbá kutatást és kísérleteket hajtottam végre a vizuális megjelenítők által sugárzott rádiós jelek információtartalmának bizonyítása érdekében. [91] [92] [93] A következő 3. vizsgálat során bizonyítom a monitorok működése során létrejövő rádiófrekvenciás sugárzás tényét. A 4. vizsgálat során indikatív módon megállapítást teszek a sugárzott jelek összetevőinek változására, a megjelenített tartalommal összefüggésben. Az 5. vizsgálat során bizonyítom a kisugárzott jelek távolabbi detektálásának tényét. A 6. vizsgálat során bizonyítom az információs tartalom kisugárzásának visszaállíthatóságát. A 7. vizsgálat során megállapítom, hogy a kivetítők esetén is fennáll a monitoroknál tapasztalható rádiófrekvenciás sugárzási probléma.

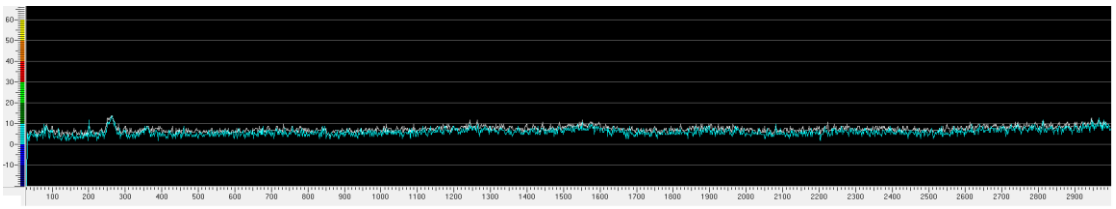
3. vizsgálat

A mérések során spektrum analizátorral történő vizsgálatot folytattam 30MHz és 3GHz közötti tartományban. A vizsgálatot három korszerű 17"-os , 19"-os és 21" -os TFT (Thin Film Tranzistor) technológiás monitoron végeztem, melyeket több különböző képfelbontási üzemmódban vizsgáltam. A vizsgálatot az alábbi 22. ábrának megfelelően alakítottam ki.



22. ábra: Monitor rádiófrekvenciás sugárzásának mérése
Forrás: saját szerkesztés

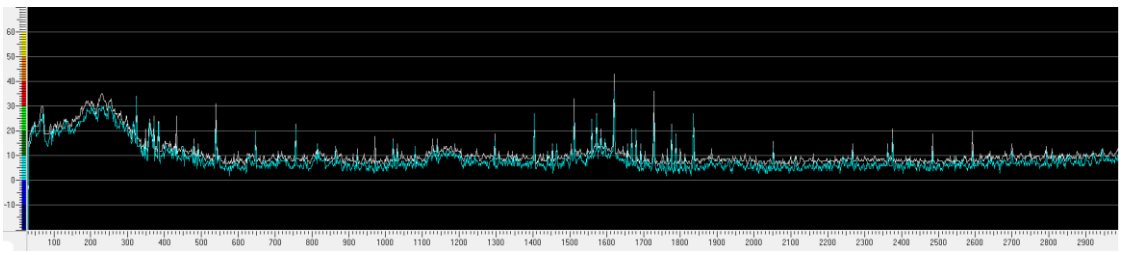
A méréseket módomban állt elektromágneses szempontból árnyékolt környezetben végrehajtani, így az alap referencia mérés zajtartalma megfelelően alacsony volt. Elsőként referencia spektrumképet vettem fel a vizsgálati mintaként szolgáló megjelenítő „minta monitor" és „monitor meghajtó számítógép" készülékek teljes áramtalanított állapotában. Az így készült, a mérőkamrában felvett referencia-spektrumfotó képe látható az alábbi 23. számú ábrán.



23. ábra Referencia rádiós környezet spektrumképe
Forrás: saját szerkesztés

A referencia felvételt követően három monitor rádiós sugárzási spektrumképét vettem fel, melyek különböző csatlakozási szabvánnyal és különböző felbontású videó jelekkel kerültek meghajtásra. A következőkben a mérések képei láthatóak, melyeken bizonyítást nyer az a feltételezés, miszerint jelentős számú, eltérő frekvenciájú jel jelenik meg a monitorok környezetében kisugárzott formában.

- Az 1. számú monitor DVI csatlakozó felület használata mellett 1280x800 pixel felbontásban a következő 24. ábrán látható spektrumképet produkálta.

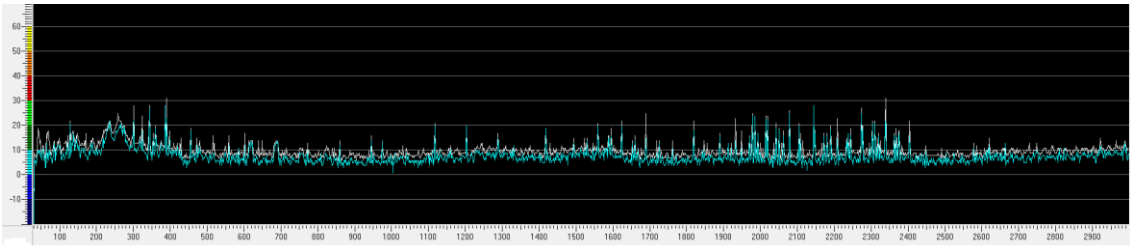


24. ábra 1. számú mintamonitor DVI 1280x800 pixel felbontású spektrumképe
Forrás: saját szerkesztés

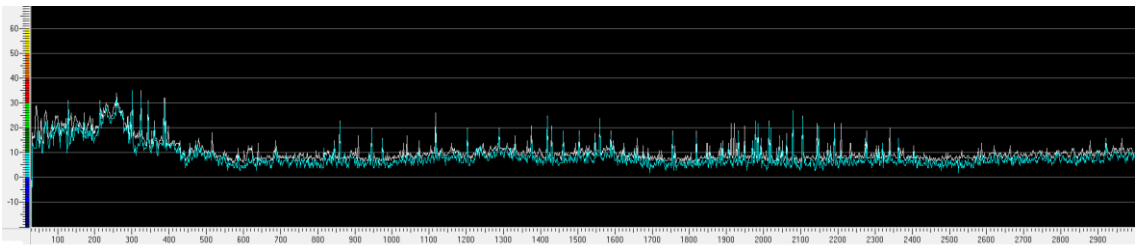
Az ábrát és a többi spektrogrammot is áttekintve rögtön szembetűnik, hogy nagy mennyiségű diszkrét frekvencia jelenik meg a rádiós spektrumban. A megjelenő frekvenciák amplitúdója eltérő. A 30MHz-től~350MHz-ig terjedő tartományban jelentős, széles frekvenciasávbeli telítődést láthatunk. Míg a 325MHz-től 3GHz-ig terjedő részben az egyedileg jól elkülöníthető frekvenciakomponensek dominálnak.

- A 2. számú monitor rádiós spektrumvizsgálata során DVI és VGA csatlakozó felületek használatával 1280x800 pixel és 1024x768 pixel felbontásban került a kisugárzás

vizsgálatra. A DVI csatlakozó felülettel végzett vizsgálatokról készült rádiós spektrumok fotója a következő 25. számú és 26. számú ábrákon láthatóak.

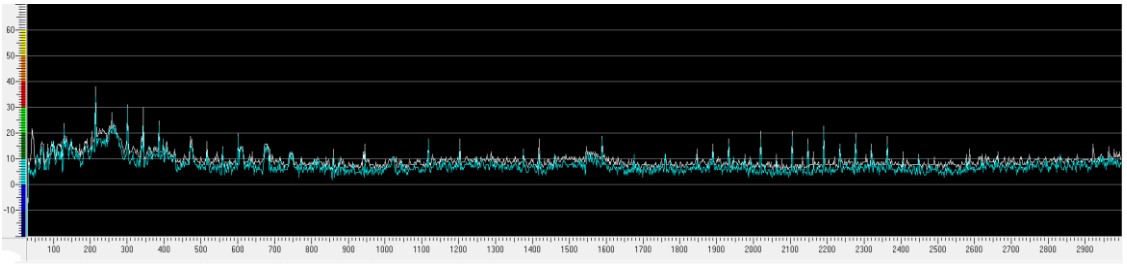


25. ábra 2. számú mintamonitor DVI 1280x800 pixel felbontású spektrumképe
Forrás: saját szerkesztés

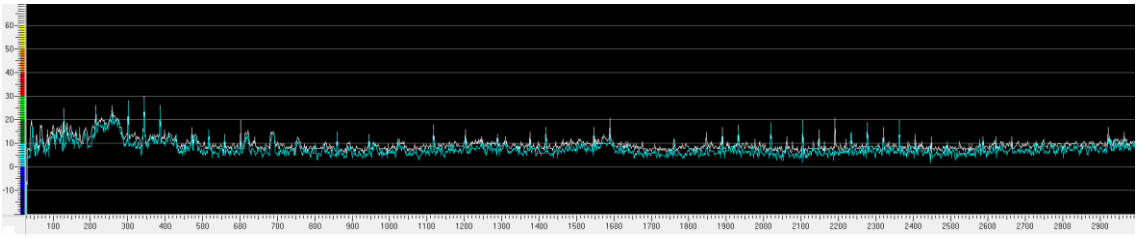


26. ábra: 2. számú mintamonitor DVI 1024x768 pixel felbontású spektrumképe
Forrás: saját szerkesztés

A VGA csatlakozó felülettel végzett vizsgálatról készült rádiós spektrumok fotója a következő 27. számú és 28. számú ábrákon láthatóak.



27. ábra 2. számú mintamonitor VGA 1280x800 pixel felbontású spektrumképe
Forrás: saját szerkesztés

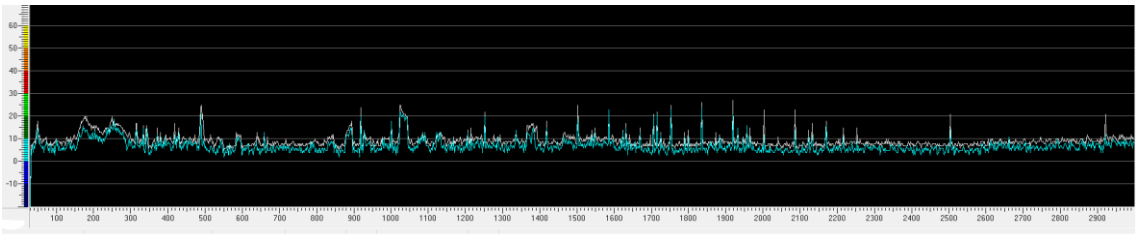


28. ábra 2. számú mintamonitor VGA 1024x768 pixel felbontású spektrumképe Forrás: saját szerkesztés

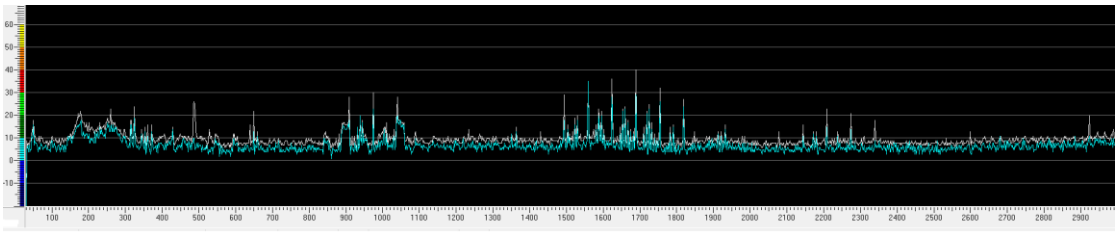
Az ábrákat összehasonlítva az első mintamonitorhoz képest, hasonlóan jól detektálható nagy amplitúdójú diszkrét frekvenciaértékek jelenlétét tapasztalhatjuk. A működés

során kisugárzott frekvenciaértékek majdnem a teljes vizsgált spektrumban jelen vannak.

- A 3. számú mintamonitort megvizsgálva DVI csatlakozó felület mellett 1280x800 pixel valamint 1024x768 pixel felbontásban mutatom be a készített spektrumképeket. A készített spektrumfotók képe a 29. számú és 30. számú ábrákon látható



29. ábra: 3. számú mintamonitor DVI 1280x800 pixel felbontású spektrumképe
Forrás: saját szerkesztés



30. ábra 3. számú mintamonitor DVI 1024x768 pixel felbontású spektrumképe
Forrás: saját szerkesztés

Ebben az esetben a monitor meghajtó jelének állítását követően a megjelenő frekvencia értékek nagyon eltérő spektrumképet mutatnak, azonban a kisugárzott rádiófrekvenciás jelek frekvenciaértékei a vizsgált sávban továbbra is nagy számban vannak jelen.

3. értékelés

A vizsgálat során bebizonyosodott, hogy a védett helyiségek kialakítása kapcsán további relevanciával bír az elektronikus vizualizációs eszközök működése során megjelenő kisugárzott rádiófrekvenciás jelek védelme. Az általánosan használt monitor megjelenítők működéséből fakadóan, a készülékek környezetében rádiófrekvenciás jelek hullámai jelennek meg.

4. vizsgálat

A megjelenő rádiós jelek vizsgálata során felmerült a jelek változásának kérdése, miszerint a monitoron lévő megjelenési kép változásának következtében változnak-e a kisugárzott jelek, korrelációt keresve a megjelenő kép információtartalmával.

A monitorok kisugárzási frekvenciáit egyesével vizsgálva, a megjelenő rádiós jelek

túlnyomó része tartalmaz valamilyen modulációt. A spektrumanalizátor beépített szelektív vevőjét felhasználva AM és FM demodulátor fokozatok kimeneti jelének vizsgálatát végeztem. Indikatív jelleggel a demodulátor kimenetére oszcilloszkópot és hangszórót kapcsoltam. A monitorokon nagy fehér kitöltésű, majd nagy sötét kitöltésű információ tartalmú állóképet megjelenítve, a kisugárzott jeleket frekvenciánként külön-külön megvizsgálva, a demodulátor fokozat kimenetének vizsgálatával, periodikus jelformákat jelenítettem meg. A monitoron megjelenített képek változtatása során, a demodulátor fokozatról vett jel jellemzői változtak. A csatlakoztatott oszcilloszkópon, valamint a hangszórón is változás volt megfigyelhető és hallható.

4. értékelés

Az elvégzett indikációs kísérlet eredményei alapján, a monitorok kisugárzott jelei túlnyomó részt a megjelenített képpel összefüggésben lévő modulált formában jelennek meg. Ugyan a mérés során nem mindegyik a frekvenciasávban vizsgált jel esetén volt tapasztalható a megjelenített kép váltásával előidézett demodulációs változás, azonban a megjelenő jelek lényeges többségében igen. A megjelenítő monitorok képernyőképének változásával korreláló rádiófrekvenciás jelek tartalmának változása elsődlegesen bizonyítja a kisugárzott jelek összefüggését a megjelenő képi tartalom kisugárzásával, ezzel lehetséges információszivárgási csatornát teremtve.

5. vizsgálat

A megjelenő jelek tekintetében szükségesnek tartottam megvizsgálni, hogy azok távolabbról, más környezetben is detektálhatók-e. A monitort és a meghajtó számítógépet a mérőlaborból egy hagyományos irodai környezetbe helyeztem. A monitoron a mérőkabinban létrehozott képpel azonos képet hoztam létre, ezzel azonos sugárzási paramétereket teremtve. A mérővevőt az új környezettel szomszédos iroda helyiségbe telepítettem. Az előzőekben a laboratóriumi körülmények között feljegyzett frekvenciatüskéket keresve néhány frekvencia jelenléte távolabbról is detektálható volt. Az indikatív mérés szempontjából negatív befolyásoló tényezőt a kis sugárzási teljesítmény, az alapzaj megemelkedése, valamint az irodai környezetben jelen lévő vezeték nélküli kommunikációs technológiák és távoli rádió adók jeleinek jelenléte jelentette. Ezen összetevők nagyságrendekkel nagyobb szinttel jelentek meg a mérőműszer skáláján a laboratóriumban tapasztaltakkal szemben.

5. értékelés

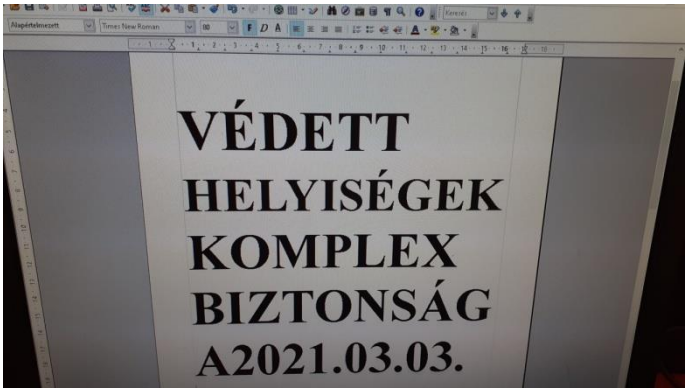
A vizsgálat során bebizonyosodott, hogy a védett helyiségek kialakítása kapcsán további relevanciával bír az elektronikus vizualizációs eszközök működése során megjelenő kisugárzott rádiófrekvenciás jelek védelme. Az általánosan használt monitor megjelenítők működéséből fakadóan, rádiófrekvenciás jelek hullámai jelennek meg a készülékek környezetében, amelyek a körülvevő tágabb környezetben is detektálhatóvá válnak. A vizsgálat során bebizonyosodott, hogy a védett helyiségek kialakítása kapcsán relevanciával bír a kommunikációs környezetben megjelenő, információ tartalmú rádiófrekvenciás jelek terjedésének megakadályozása.

6. vizsgálat

A monitor képmegjelenítők működése során kisugárzott jelek információtartalmának vizsgálatával kapcsolatban, az irodalmi forráskutatás elemzése során egy érdekes, a témához szorosan kapcsolódó kutatás eredményét találtam. A Cambridge Egyetem kutatója Martin Marinov 2014-ben publikálta doktori értekezését, amely „Remote video eavesdropping using a software-defined radio platform" [5] címmel jelent meg. [94] Az értekezés témája, valamint a publikált megoldás témához való kapcsolódása megerősítette a vizsgálatok folytatását. Az értekezés eredménye és az ismertetett vizsgálathoz szükséges hardver és szoftverkörnyezet elérhető volt. A célszoftver [6] a github.com oldalon található. A számítógép monitorok üzemszerű működése során keletkezett rádiós jelek információtartalmának vizsgálatát, újabb indikatív módszerrel, saját műszeres és mérési környezetben megvalósítottam. A mérési környezet megfelelt a 22. ábra „Monitor rádiófrekvenciás sugárzásának mérése" ábrán kialakított elrendezésnek. Az ábrához képest a mérő rendszer vevő berendezését a spektrumanalizátor helyett egy HackRF ONE SDR (Softwer Defined Radio)-ra kellett cserélni. A vezérlő program Windows operációs rendszer alatt futott. [95] Az indikáció elvégzéséhez a „TempestSDR" program szimulációs környezete került kialakításra az SDR vezérlő számítógépen. A megfelelő összeállítás után a demonstrációs kísérletet elvégeztem. A vizsgálathoz a 2. számú mintamonitort használtam, amelyhez a következő 31. ábrán bemutatott meghajtó videó jelforrás képét állítottam be.

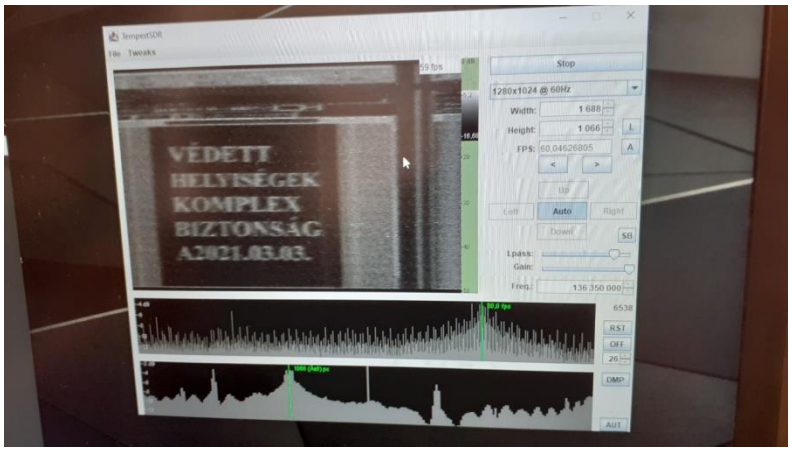
[5] forrás:https://github.com/martinmarinov/TempestSDR/blob/master/documentation/acs-dissertation.pdf

[6] https://github.com/martinmarinov/TempestSDR/tree/master/TempestSDR



31. ábraA számítógépes monitor megjelenítők által sugárzott rádiós jelek információtartalmának vizsgálatához használt jelforrás képe
Forrás: saját szerkesztés

A kép beállítását követően megvizsgáltam a megjelenő rádiós jeleket. A monitort 1280x1024 pixel felbontásban meghajtva, 136,3MHz-en markáns rádiós jel jelent meg. A célprogramban a frekvenciát beállítva, a finomhangoló egységeket állítva, a sugárzó monitor képe megjelent a vételi oldalon lévő számítógép képernyőjén. A megjelenített kép képernyőfotója a következő 32. ábrán látható.



32. ábra A TempestSDR programmal megjelenített monitorkép visszaállítás képernyőfotója
Forrás: saját szerkesztés

Az indikációs kísérletet mérőlaborban sikerült reprodukálni.

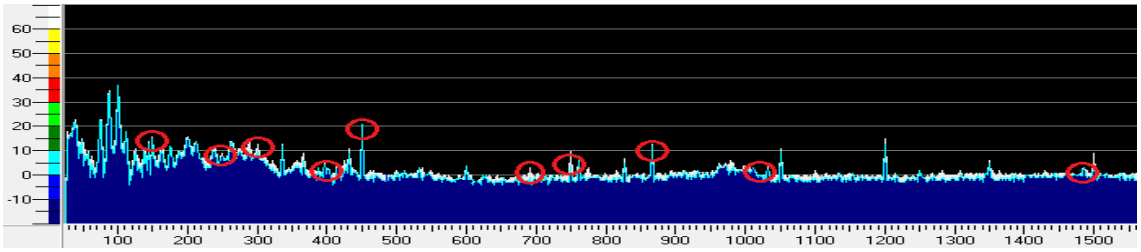
6. értékelés

A monitor megjelenítők által sugárzott rádiófrekvenciás jelek információbiztonsági vizsgálatának látványos eredményeként indikálással szemléltettem, hogy saját műszerekkel végzett ismételt kísérlet alapján, az információbiztonsági rés a gyakorlatban is fennáll. A kísérlettel szemléltettem, hogy a monitorok által sugárzott

jelekből a kép visszaállítható, így a védett helyiségek szempontjából, az elvi rések kiküszöbölésére tett intézkedések kialakítása, és a védelem kialakítása során tett ellenintézkedés szükségessége megkérdőjelezhetetlenné vált.

7. vizsgálat

A megjelenítők elemzése kapcsán, felmerült a videó kivetítő projektorok rádiófrekvenciás kisugárzásának vizsgálata. A méréseket folytatva megvizsgáltam egy kivetítő berendezést, melynek környezetében az alábbi 33. számú ábrán látható rádiófrekvenciás jelek voltak kimutathatóak. A kisugárzott jeleket vizsgálva, tíz frekvenciasávot azonosítottam, melyeknek jelei, korreláltak a megjelenített kép változásával. Ezek a 148,5MHz; 247,51MHz; 296,98MHz; 396MHz; 445,6MHz; 683,1MHz; 742,5MHz; 870MHz; 1039,5MHz; 1484,9MHz frekvenciák környezetében voltak kimutathatóak.



33. ábra Video kivetítő projektor rádiós spektrumbeli kisugárzásai, a megjelenített képpel korreláló jelek megjelölésével
Forrás:saját szerkesztés

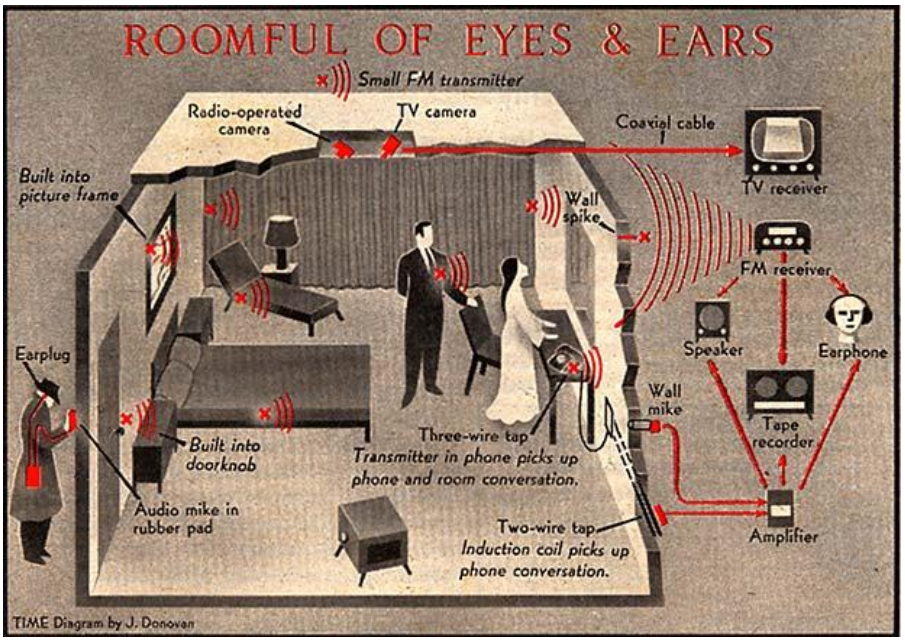
7. értékelés

A videó kivetítő projektorok és a monitorok esetében is tapasztalható rádiófrekvenciás jelek sugárzásából eredő információbiztonsági probléma.

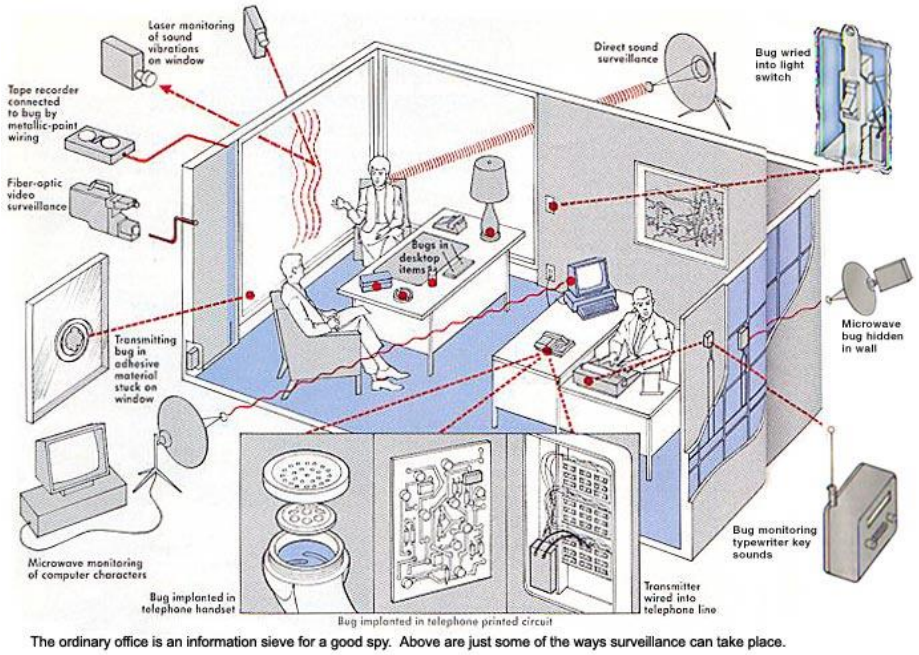
4.2 Helyiségeket érintő offenzív technikai fenyegetettségek

Az előző alfejezet példái, saját kísérletek alapján indikálják és bizonyítják a kommunikáció során megjelenő információt hordozó fizikai jelenségek támadhatóságát. A források elemzése kapcsán további két szemléletes grafikus ábrát építettem be, amelyek tovább alapozzák a védett helyiségek kialakítása során alkalmazott defenzív megoldások megfelelő struktúráját. A 34. számú ábra az 1960-as évek, míg a 35. számú ábra az 1980-as évek technikai színvonalát szemlélteti. Az ábrákon támadó jellegű, helyiség-megfigyelésre alkalmazott technológiák képei láthatóak. A korábbi ábra a

tranzisztorizálás hajnalán készült, amely példái túlnyomó részt az analóg vonalas hozzáférésű technológiák és az egyedi rádiós adók kialakítását jelenítik meg. A technológiák elemei mai szemmel nézve nehézkes, nagyméretű alkotókból állhattak, feltételezésem szerint hibrid elektroncső és tranzisztoros áramköri elemekből épített készülékekkel. A tápellátásuk hálózati energiaellátást igényelt, a korai autonóm energiaforrások korlátos teljesítménye miatt.



34. ábra A technikai hírszerzés lehetőségei a 60-as években Forrás: [96]; [97]



35. ábra A technikai hírszerzés lehetőségei a 80-as években Forrás: [96]

A 35. ábrán, kifinomultabb technikai támadási módszerek megvalósítása látható. Az ábrát megvizsgálva legalább 13 technikai fenyegetés jelenik meg, amely a technika fejlődésének arányában korszerűbb eszközöket és az előzőhöz képest új módszereket feltételez. Az ábrákon megjelenő eszközöket a megszerezni kívánt információ szempontjából több csoportra oszthatjuk, amelyek részletes feltérképezése alapvető információt nyújt a védett helyiségek megfelelő kialakításához.

Az érzékelt fizikai jellemzők szerint csoportosítva:

- helyiségben elhangzó audio információ elsődleges és másodlagos fizikai jelenségeken alapuló detektáló eszközök:
    - vezetékes akusztikus érzékelő (átvitel: külön vezeték, energia ellátó hálózat vezetékei)
    - vezeték nélküli elemes táplálású akusztikus rádióadó
    - vezeték nélküli elemes táplálású akusztikus rögzítő
    - hálózati táplálású akusztikus rádióadó
    - parabolikus akusztikus érzékelő
    - kontakt akusztikus érzékelő
    - lézer akusztikus érzékelő
    - mikrohullám táplálású akusztikus adó
    - hálózati táplálású helyben működő akusztikus érzékelő
- helyiségben megjelenő vizuális információt detektáló eszközök:
    - száloptikai kamera
    - vezetékes táplálású kamera
    - vezeték nélküli, elemes táplálású kamera rádióadó
    - helyben - helyiségben működő videó rögzítő
    - hálózati táplálású - helyiségben működő videó rádióadó
- helyiségben működő elektronikus eszközök működése során indirekt formában megjelenő információt detektáló eszközök
    - billentyűzet leütésének hangját figyelő eszköz
    - vezetékes telefon induktív csatoló eszköz
    - megjelenítő monitor másodlagos, elektromágneses kompromittáló sugárzását érzékelő detektáló eszköz

A források elemzése kapcsán a fizikai indikációs kísérletek helytállónak bizonyulnak, mivel a témafeldolgozás közben megjelenő források hasonló irányba mutatnak.

A tézis igazolásának részeként, kitekintést végeztem a kereskedelmi forgalomban megjelenő, fenyegetést jelentő technikai eszközök irányában. A kapcsolódó internetes keresés számbeli eredményeit elemezve, több tízezer, esetenként több milliós találati eredményt kaphatunk a téma kapcsán szóban forgó berendezések magyar és angol megfelelőinek szinonimáira. Egy keresési minta eredményét az 3. számú táblázatban láthatjuk. A felhozott találatot és kínálatot áttekintve látható, hogy egy egész iparág épült a témában meghatározó berendezések gyártására, a készülékek teljes arzenálját alkotva. Az eredmények magas százaléka kereskedelmi jellegű, így szabad vásárlási lehetőséget adva a termékek iránt érdeklődőnek és fokozott veszélyeztetettséget teremtve az elhangzó és megjelenő információ bizalmasságára.

Kereső kifejezés	**Google találat**
spy bug (kém eszköz)	56.400.000
eavesdropping bug (lehallgató eszköz)	8.780.000
FM bug (FM eszköz)	43.100.000
covert video surveillance (rejtett videó megfigyelő)	12.700.000
wireless mini camera (vezeték nélküli mini kamera)	357.000.000
wireless spy camera (vezeték nélküli kém kamera)	29.000.000
wireless spy transmitter (vezeték nélküli kém adó eszköz)	60.500.000
wired spy transmitter (vezetékes kém adó eszköz)	8.690.000
GSM bug (GSM eszköz)	9.180.000
lehallgató berendezés	27.800
titkos megfigyelő berendezés	74.500

3. számú táblázat Internetes keresés alapján adott Google találatok száma

Forrás: saját táblázat; (2021.03.)

A könnyű hozzáférhetőség fokozott biztonsági kockázatot jelent a hagyományos fizikai védelmi metódusokkal kialakított, többnyire őrzött biztonsági helyiségek tekintetében, mivel azok jórészt csak a vagyonvédelem elemeit tartalmazzák. [74] [98] Ezúton ismételten felhívom a figyelmet, hogy a tárgyalt eszközök alkalmazásának feltétele, törvény által meghatározott, így azok engedély nélküli használata büntető eljárást von maga után. [20] [59]

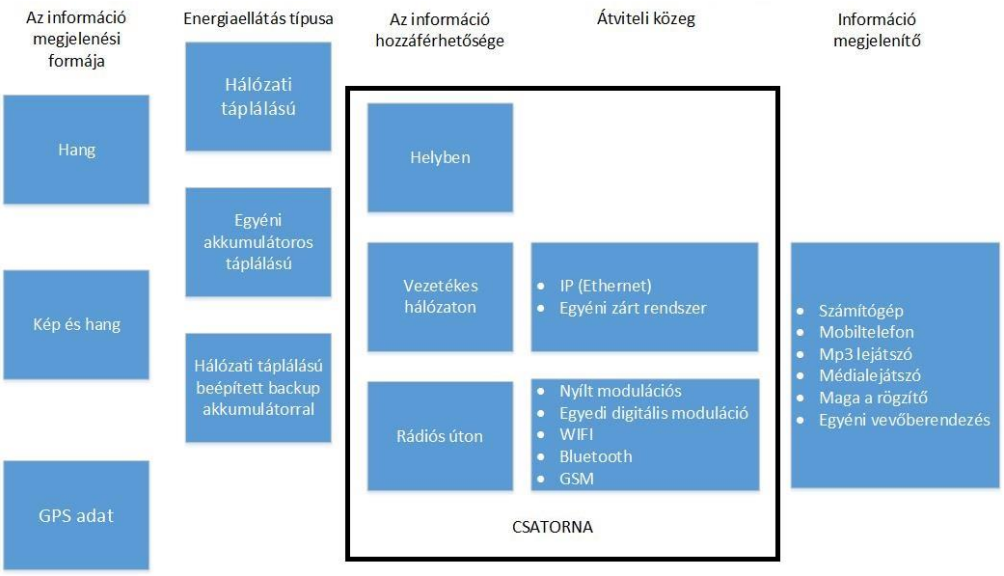
A forráskutatás során, egy technikai ellenőrző eszközöket gyártó cég nemzetközi szimpóziumán, számos támadóeszköz került bemutatásra, amelyek összefoglalója a 36. számú ábrán látható.

36. ábra Támadó eszközök összefoglaló ábra Forrás: [99]

Az internetes piacon található eredmények valamint a szimpózium forrásban bemutatott eszközök, paramétereiket tekintve nem specializált szélsőséges fizikai paraméterek megfigyelésére készített berendezések (mint például rádiós kisugárzás, tárgyakban terjedő hangrezgések), hanem inkább elsődlegesen megjelenő audiovizuális tartalom direkt megfigyelésére. A következőekben a kutatás során, katalógusadatok alapján megvizsgált eszközök paramétereinek csoportosítását mutatom be, a védett helyiség megfelelő kialakítása érdekében.

4.3 A helyiségekben megjelenő információra fenyegetést jelentő szabadpiaci eszközök csoportosítása az ellenük való intézkedések megalapozásához

A készülékek műszaki jellemzőinek feldolgozása során, egy olyan csoportosítás volt a cél, amelyben tisztán látható a készülék által megfigyelhető információforrás formája, a működéshez szükséges energia ellátása, a megfigyelés során keletkezett adatok hozzáférhetősége, az átviteli út (csatorna) és a megfigyelt közeg technikai megjelenítési formája. Cél a vizsgált eszközöknél a Shannon - Weaver hírközlési modell átvitel csatornájának a meghatározása, a védett helyiség kialakítása során alkalmazható csatorna blokkolás megállapítására. A csoportosítás a 37. számú ábrán látható.



37. ábra Az interneten található információrögzítő berendezések osztályozása működés szerint
Forrás: saját szerkesztés

Az elemzés alapján látható, hogy a megfigyelni kívánt fizikai információk, amelyeket az áttanulmányozott berendezések érzékelni képesek, három alapparaméter köré tagozódnak. Kép, hang és földrajzi koordináta, valamint ezek kombinációi. Jelen esetben a védett helyiségek biztonságát illetően a hang és képi események érzékelésére alkalmas berendezések elemzése a mérvadó, azonban a GPS adat érzékelésére alkalmas eszközök új vetületet teremtenek az információbiztonság megteremtése kapcsán. A GPS nyomkövetőkkel kapcsolatos felvetéseket a kutatás keretein belül nem tárgyalom.

A berendezések energiaellátása szempontjából megvizsgáltam azok elektromos táplálását. Az elemzett eszközök három csoportba sorolhatók, melyek befolyásolják a feltételezhető működés idejét. A csoportok elemei lehetnek elektromos hálózati táplálásúak, egyéni akkumulátoros-elemes táplálásúak, valamint hálózatról működő az időszakos energia kiesést saját beépített akkumulátorról áthidaló típusok. Az információbiztonsági rést jelentő, érzékelt-rögzített adatokhoz való hozzáférés szempontjából szintén három csoportba sorolhatók az eszközök.

Helyben tároló típus. Itt önálló szigetüzemről beszélhetünk. Ezek az adatrögzítők elhelyezve a típusuknak megfelelően magukon tárolják a rögzített eseményt. A rögzített információhordozóhoz való hozzájutáshoz szükséges az eszközhöz történő újbóli hozzáférés.

A következő típuscsoport, amelynek adattartalma, illetve információtovábbító képessége távolról is elérhető. A hozzáférés kialakítástól függően lehetséges vonalas, vagy rádiós megoldás. Az oszlop második és harmadik halmazcsoportjában lévő

berendezések üzeme során, nem szükséges a berendezéshez való állandó fizikai hozzáférés, elég egy egyszeri installálás. Párhuzamot vonva gondoljunk egy biztonsági kamerarendszer kiépítésére és az azzal járó kiépítési feladatok elvégzésére. Feltehetően az említett berendezések elhelyezése bonyolult, de az üzembiztonságuk szempontjából stabilak. Az elemzett berendezések által alkalmazott átviteli közeg alapján, a rádiós csoportba sorolt készülékeket megvizsgálva, az alapnak számító analóg modulációs eljárástól, napjaink telekommunikációs szabványainak megfelelő rádiós kommunikációs eljárásokig, szinte a teljes paletta megtalálható. Az egyéni analóg, vagy saját modulációs eljárással rendelkező adó hallhatósági hatósugara nagyban függ az adó kimenő teljesítményétől. A WLAN, Bluetooth valamint GSM kialakítás esetén a hatótáv tekintetében a technológia szabványára jellemző teljesítményviszonyokkal számolhatunk. A rádiós hírközlési szabványokat támogató berendezések önálló elérhetőségi távolsága az adó teljesítményének növelésével ugyan nem növelhető egy bizonyos mértéken túl, azonban, ha rendelkezésre áll szabványos telekommunikációs hálózat, arra csatlakoztatva szinte bármilyen távolságból elérhetővé válnak.

A csoportosított tulajdonságok hozzáférhetőség és átvitel elemei a Shannon - Weaver modell csatornája, ahol a védett helyiségek kialakítása kapcsán a blokkolást célszerű megvalósítani.

Az elemzett berendezések által továbbított vagy rögzített információ formátuma mára már kizárólag digitális jellegű lett az analóg technikákat háttérbe szorítva, így az információs tartalom megjelenítése, a szokványos digitális médialejátszást támogató berendezésekkel lehetséges.

A témában mérvadó, fenyegetést jelentő szabadpiaci eszközökhöz történő hozzáférés lehetőségét kronológiai szempontból vizsgálva, az internet előtti időszakban a szóban forgó berendezések általános polgári beszerzése gyakorlatilag lehetetlen volt. A kutatás során felismert tények azt mutatják, hogy a technológia rohamos fejlődése, az árak rohamos csökkenése és a szabadpiac miatt a hozzáférés korlátlanná vált.

A média csatornáinak hírközléseit elemezve feltételezhető, hogy az információk védelmére tett hagyományos fizikai, logikai és IT biztonsági intézkedések erősödése miatt, eltolódás várható az információszerzés módszerei tekintetében a tárgyalt eszközök irányába. [100] [101] [102]

4.4 SMART folyamatok

A kutatás interdiszciplináris folyamata révén kitekintést tettem a SMART folyamatok és a védett tárgyaló kapcsolatára, miszerint a technika fejlődésével egyre több infokommunikációs eszköz lepi el a mindennapi életünket. [103] A megjelenő folyamat támogatja a kommunikációs eszközök terjedését, ezzel növelve a védett helyiségek falai közé bevinni kívánt információbiztonsági rések számát. Századunk technikai fejlődése, olyan mértékű változást hozott az emberiség életébe, amely a mindennapi életet gyökeresen megváltoztatta. Az információs infrastruktúrák szaporodásával az informatikai és kommunikációs rendszerek berendezései teljes mértékben beleszövik magukat életünkbe, ezzel megkönnyítve a társas érintkezést, az üzleti életet valamint a mindennapi információs szükségleteink igényének kielégítését. Miután az emberiség nagy része városokba rendeződve éli mindennapjait, kézenfekvő, hogy a városi környezet, mint élettér kedvez az infokommunikációs technikai vívmányok elterjedésének lefedve a teljes életteret. Új típusú szolgáltatói csoportok jelennek meg, akik az infókommunikáció legújabb trendjeit kínálják.

4.4.1 A SMART-osodás és a biztonság ellentmondása

A témához kapcsolódóan saját megközelítés alapján meghatároztam az okos tárgyaló fogalmát:

Okos tárgyaló (saját kifejezés), olyan a kor követelményeinek megfelelő, az ember-ember közötti személyes és távoli kommunikációt segítő technológiákkal és technikákkal felszerelt helyiség, ahol a legmodernebb informatikai berendezések és technológiai elemek mellett a kényelmi, ergonómiai funkciók is párosulnak a minél eredményesebb és kényelmesebb kommunikáció megvalósítása érdekében.

Mivel az okos eszközök és az információs technológiák szerves részét képezik az életünknek, így az azokkal megjelenő biztonsági kockázatok is napi szintű problémává váltak, mind a magán, mind a vállalati környezetben. [104]

Az információs technológiák nélkülözhetetlenné váltak a munkahelyeken, viszont ezzel szemben a gazdasági érdekek sokszor az információk bizalmasságát és védelmét kívánják meg. Az okos városok okos tárgyalói egy ellentmondásos helyzetet teremtenek a védelmi intézkedések kidolgozása szempontjából, mivel követik az információs eszközök terjedésének és beépítésének a trendjeit, azonban a sebezhetőség ezzel arányban nő. A CSIC (Center For Strategic & International Studies) összefoglalója

alapján jelentős mennyiségű kiber incidens került rögzítésre 2006 és 2020 között, mely az alábbi 38. számú ábrán látható. Azon kiber incidensek kerültek rögzítésre, melyek a kormányzati szerveket, védelmi és csúcstechnológiai társaságokat érintettek, és [105] több mint egy millió dollárt meghaladó veszteséget okoztak.

38. ábra Jelentős kiber támadások országokra vetített statisztika alapján
Forrás: [106] alapján

Előfordulhat, hogy egy újabb berendezés vagy rendszer előre nem látható biztonsági rést hordoz magában, kellemetlen meglepetést okozva a felhasználói számára. [107] Olyan biztosított környezetben, védett helyiségben kell a bizalmas társas kommunikációt megvalósítani, amely garantálja, hogy a kommunikáló felek interakciója csak a meghatározott részvevők számára válhasson ismertté. A technológiák ismert sebezhetőségéből kiindulva nem elég a kommunikációban résztvevő felek bizalmi és titoktartási vállalása, hanem egy olyan helyiségben kell az információk cseréjét létrehozni, amelyből a harmadik fél információhoz való jutását kizárjuk. Az információs és kommunikációs technikákkal lefedett munkahelyi környezetet elképzelve, csakis védett tárgyaló jellegű helyiségekben valósítható meg az ilyen védett emberközeli diskurzus. [73] [108] [109] [110]

4.4.2 Az okos tárgyaló és az információbiztonság

A témán elgondolkozva jogosan tesszük fel a kérdést: Mitől válhat okossá egy tárgyaló? Az ergonómiai és fiziológiai kialakítás, a kényelem, és a beépített vizualizációs, valamint infokommunikációs technika tesz okossá egy tárgyalót. Minél több és jobb a beépített technológiák mennyisége, annál okosabbnak mondható.

A kommunikációs funkciókat külön-külön kielemezve, elsődleges a prezentálni és megbeszélni kívánt tartalom könnyű megosztása audio és vizualizációs technika segítségével. Itt különböző kivetítők, okos táblák és monitorok megjelenésére gondolhatunk. Könnyen elképzelhetjük, hogy lassan a google szemüvegek és háromdimenziós megjelenítők világában rohamosan beépülnek a tárgyalók falai közé az említett eszközökhöz hasonló tudású berendezések. Ezek alapfunkcióit tekintve hálózati végberendezésként üzemelnek az internetet, mint szükséges működési alapfeltételt igényelve. Nem elég az energiaellátás biztosítása a funkciók eléréséhez, az internet is mint szükséges alapszolgáltatás rendelkezésre kell, hogy álljon. Ezzel egy nagysebességű adatátviteli közeget telepítve a helyiség falai közé. A felgyorsult világ nem engedi meg tárgyalások nagymértékű késleltetését távoli döntéshozó személyek érkezésére várva, így funkcióit tekintve a távoli résztvevőkkel történő kommunikáció megvalósíthatósága szintén alapvető funkciója a SMART tárgyalók beépített funkciójának. Továbbá alapfeltétel a mindennemű infokommunikációs technika rendelkezésre állása, a vezeték nélküli és mobiltechnológiák teljes lefedettsége mellett. A tárgyalások gyakran jegyzőkönyv írását kívánják meg, így hang és képfelvétel készítését is, amelyre általában stúdióba rendezett eszközrendszert építenek be. A kényelmi és ergonómiai elemek nagy hangsúllyal vannak jelen a korszerűnek mondható tárgyalókban, akár a hangvezérelt gépészeti és árnyékolástechnikai eszközöket vesszük alapul, akár a klíma berendezések vezérlését.

Ha tisztán az infokommunikációs technikákat vesszük vizsgálat alá, akkor az alábbi technológiákkal és az egyenként hozzájuk tartozó biztonsági résekkel találjuk szembe magunkat:

- Internet végpontok bevezetése egy külső helyiségből
- Vezeték nélküli hálózat (WLAN)
- Konferencia berendezés
- Kihangosító berendezés - stúdióval

- Tolmács berendezés - stúdióval
- Beépített videó megfigyelő rendszer
- Fix telepítésű és hordozható számítógép
- Kivetítők, monitorok
- Vezeték nélküli konferencia szoba vezérlő
- GSM lefedettség az összes technológia tekintetében

Az imént felsorolt technológiai elemekkel ellátott tárgyaló és egy védett helyiség funkcióit tekintve nagyon eltérnek egymástól. A védett helyiség biztonságát az egyenszilárdság és az ellenőrizhetőség elvei alapján kell kialakítani. Véleményem szerint egy okos tárgyaló nem igazán lehet védett tárgyaló a technológiai trendek beépítésével. A kivetítők, beszéd kihangosítók, videó-konferencia rendszerek alkalmazása védett helyiségekben a magukban hordozott biztonsági kockázatok miatt lehetőség szerint kerülendő megoldások. Javaslatom alapján a védett tárgyalók információbiztonsági megközelítését az alábbi szempontok szerint kell megközelítenünk:

- fizikai biztonság
- elektronikus információbiztonság
- dokumentumbiztonság
- kimondott szó biztonsága
- megjelenő vizuális információ védelme
- a kommunikáció során létrejövő, információtartalmú fizikai jelenségek védelme

A felsoroltak közül az első három rendelkezik kialakult, a vagyonvédelem kialakításához használt kész megoldásokkal, viszont a kimondott szó és a megjelenő kép - vizuális tartalom valamint azok megjelenése során létrejövő fizikai hatások védelme a fejezet előző részeiben valamint az előzőekben felvázolt igények kontextusában védelmi intézkedések kialakítását kívánja meg. [111] [17] [71] [112] [113]

4.4.3 Védett tárgyaló optimalizálása

Az okos tárgyalóknál alkalmazott technológiák biztonsági réseit szemügyre véve egy védett tárgyaló csak korlátozott módon lehet okos tárgyaló. Bizonyos

kompromisszumokat kell kötnünk a kényelemi megoldások és a tárgyalókban alkalmazott infokommunikációs technológiák alkalmazását illetően.

A vizualizációs megoldások közül, csak olyan hardvert szabad a tárgyaló falai közé vinni, amely fizikálisan, hozzáértő szakember által ellenőrzött készülék, ellenőrzött szoftver környezettel. Abban a működéshez szükséges alkatrészeken kívül más alkatrész nincs. Az ellenőrzés ténye és érvényessége garantálható kell, hogy legyen.

Amennyiben lehetséges további technológia minimalizálásra van szükség egy védett helyiség tekintetében. A helyiség falai között ne legyen fixen telepített adatkapcsolati technológia. Amennyiben nélkülözhetetlen egy védett helyiség kialakítása során az IT adatátvitel kialakítása, akkor azt elképzelésem szerint a harmadik fejezet 7. ábráján bemutatott adminisztratív zónában kell elhelyezni.

A védett helyiség kialakításához kapcsolódóan szakirodalmi kutatást végeztem az IT adatátviteli technológiák fizikai közegeinek területén. A vizsgálódás eredményeként megállapítottam, hogy a lehetséges technológiák közül az optikai szál kialakítása a legmegfelelőbb. Az alkalmazása révén szálfelügyeleti berendezés alkalmazása válik lehetővé, mellyel azonnali hibabehatárolás, valamint száljellemző változás detektálható. A témát a következő fejezet kapcsolódó részében fejtem ki. [72] [114] [5]

ÖSSZEGZÉS

A fejezetben a negyedik és ötödik hipotézisem kerül vizsgálatra. A fejezet elsődleges céljaként elméleti csoportosítást végeztem a hírszerzés módszereinek tekintetében. Csoportosítottam az elektronikus információszerzés elemeit és kommunikációs útjait, melyek fenyegetést jelenthetnek a védett helyiségben megjelenő információra. Felvetésem alapján csoportosítottam a téma szempontjából lényeges támadási módokat, aminek következtében megállapítható a kutatás további irányvonala a védelmi intézkedések kialakítása. A kutatási irány sokrétűsége miatt áttekintettem az emberi kommunikáció folyamatát és a megjelenő fizikai jelenségek sorát, melyek eredetének ismerete szintén hozzájárul a védelmi kialakítás megvalósításához. A kommunikációs folyamat elvi bemutatása után demonstratív gyakorlati méréseket végeztem az információ terjedésének és a felmerülő információbiztonsági rést jelentő folyamatok bizonyítására, melyek alapjául szolgálnak az offenzív technikai eszközök által detektálható fizikai jelenségek információbiztonsági problémájának bizonyítására.

Ezt követően ábrákon keresztül bemutatva áttekintettem az offenzív alkalmazások lehetőségeit, melyek számos támadási vektort tüntetnek fel. Osztályoztam a nyílt forrásból megismerhető helyiségellenőrzés megvalósítására alkalmas technikai eszközök paramétereit, igazolva a probléma fennállását. A kutatás során megállapítottam, hogy az internetet, mint multi-funkciós felületet kihasználva, olyan technológiai és információszerzési indirekt felület is elérhető, amely a világháló előtti világban szinte elképzelhetetlen lett volt. Az adatrögzítő - továbbító technológiák fejlődésével, a technikai berendezéseink mérete exponenciális mértékben csökkent, már-már szinte a kézzel alig fogható méretre. A rögzítő technológiák méretcsökkenésével az információrögzítő hardverek mérete is arányosan csökkent. Így lehetőséget biztosítva rejtett információszerzés megvalósítására. A fenyegetést jelentő elektronikai eszközök fő paramétereinek megismerésével, és azok csoportosításával megjelölhető az a pont, ahol a működés meggátolható, vagyis kialakítható egy olyan környezet, amely valahol az alkalmazhatósági láncban meggátolja az adott berendezés működését, vagy aránytalanul megnöveli az információszerző technológia alkalmazására fordított befektetés mértékét. Akusztikus demonstráló mérésekkel igazoltam a hangrezgések terjedését a határoló környezetben az információbiztonsági szivárgási csatorna bizonyítása érdekében. Optikai kísérlettel igazoltam a vizuális tartalom távoli megjelenését. Rádiós mérésekkel igazoltam a megjelenítő eszközök nem

üzemszerű rádiófrekvenciás sugárzásait. A kutatás során, saját eszközökön végzett, átvett kísérlettel igazoltam a kompromittáló elektromágneses sugárzásból eredő jel alapján történő képvisszaállítás tényét, amely egyértelműen igazolja a védett helyiség rádiós árnyékolásának szükségességét. Kísérleteim alapján megállapíthatóak azok a műszaki megoldások, amelyek defenzív hatással vannak a védett helyiségekben létrehozott kommunikációs folyamatra. Összegzett eredményeim azt is bizonyítják, hogy a védett tárgyaló biztonságát az elektronikus technikai eszközök negatívan befolyásolják. A kutatás során kitekintést tettem a SMART-osodási folyamatok irányába, melynek során megállapítottam, hogy amennyiben egy védett tárgyaló kialakítását és üzemét elemezzük, úgy komoly ellentét rajzolódik ki a SMART tárgyalók és eszközök, és a védett tárgyalók és az azokban alkalmazható megoldások között. Egy jól védett helyiség vagy tárgyaló üzemben tartása, más szemléletet kíván, mint napjaink trendje. A technológiai fejlődést háttérbe helyezve a védett helyiségek esetén, az információ bizalmasságának elérése érdekében a helyiség mindennemű ellenőrizhetőségét kell szem előtt tartani.

V. VÉDETT HELYISÉG KOMPLEX BIZTONSÁGÁNAK MEGVALÓSÍTÁSA

Jelen fejezet célja a hatodik és hetedik hipotézispontjaim vizsgálata és igazolása. A korábbi fejezetekben közölt kutatási eredmények felhasználásával összegzem a védett helyiségek fizikai kialakításának elvi sarokpontjait, a feltérképezett kockázati tényezőkre bevezetett védelmi megoldások többszintű meghatározásával. A védelmi megoldások ajánlásaival körvonalazom azon megoldások és intézkedések relevanciáját, amelyekkel elérhető a védelmi stratégiai cél, azaz a védett helyiség definíciója szerinti modell kialakítása.

BEVEZETÉS

Magyarországon a téma szempontjából mérvadó védett helyiségek tervezésére, kivitelezésére, hatékonyságának ellenőrzésére, üzemeltetésére, nyílt hozzáféréssel nem található érvényben lévő előírás. A kutatás eredményeit felhasználva a védett helyiségek fizikai kialakítása több megközelítés alapján képzelhető el, a kialakított környezetre jellemző információbiztonsági cél többszintű elérése érdekében. A védett helyiségben megjelenő humán kommunikáció során keletkező információtartalomnak helyben kell maradnia, a kommunikáció során létrejött információtartalmú fizikai jelenségek nem juthatnak tovább a határoló falazatnál. A kialakítások tekintetében beszélhetünk időszakos jelleggel kialakított, illetve megfelelővé tett térrészről, vagy egyedi kivitelű, minden technikai követelményt kielégítő állandó helyiségről. A védeni kívánt helyiségek kockázati elemeinek csökkentése során, bevezethetőek új elemek, melyek a használó személyek igényei kapcsán merülnek fel. Egy védett helyiség üzemeltetése elképzelhetetlen minőségi személyátvizsgálás és beléptetés nélkül, melynek célja az ellenőrizetlen technológiáktól mentes környezet fenntartása. A fenyegetést jelentő kockázatokat áttekintve, meghatározható a védelem mechanizmusa, amellyel a fenyegetést jelentő tényezők értéke minimálisra csökkenthető. A védett helyiségek fizikai kialakítása során törekedni kell az összes számba vehető elvi információbiztonsági rés kizárására, a maradványkockázat minimálisra csökkentésének érdekében. A védett helyiségek információbiztonsági fenyegetettségének lehetséges kockázatai és az azok ellen hozott intézkedések mennyisége lényeges szempontot képviselnek a védett helyiség kialakítása során, amely befolyásolja a kialakítás során

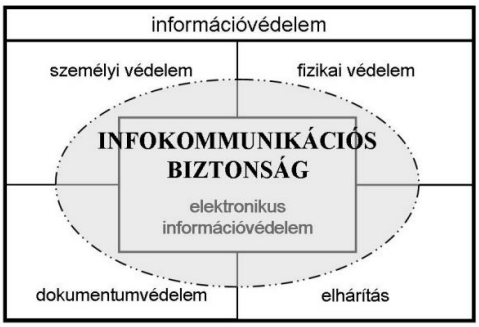
igénybe vett erőforrások számát. A védett helyiségek kialakítása és üzeme folyamatos karbantartást-átvizsgálást igényel, melynek során a helyiség jellemzőitől függő biztonsági állapot elfogadható szintre hozható vagy meghatározott szinten tartható. Kapcsolati mátrix összeállításával a művelet összetevői, valamint a kockázatot jelentő tényezők párosíthatók. A védett helyiségek átvizsgálásának elengedethetetlen része a rádiós környezet ismerete, mely kapcsán elvi áttekintést teszek a rádiós felügyelet megvalósítási módjait áttekintve. Továbbá saját elgondolás alapján megoldást adok a rádiós sugárforrások épített környezetben történő lokalizálásának megvalósítására. A helyiségen belüli prezentációs technológia kockázati jelleggel bír, azonban létrehozható olyan kompromisszumos megoldás, melynek során a technológiai szükséglet teljesíthető. A kutatás eredményeként bemutatom a védett helyiség javasolt kialakításához alkalmazható építőelemek struktúráját. A védett helyiségek kialakítása során szükségképpen felmerül a külvilág felé történő kommunikáció megteremtésének igénye, melynek ellentmondásos viszonyát kompromisszummal kezelve javaslatot teszek az átviteli technológiára, nagy hangsúlyt fektetve a fizikai réteg felügyeletének megvalósíthatóságára.

A védett helyiségek kialakításával kapcsolatban összegzem a kialakítás során figyelembe venni kívánt paramétereket, ahol egy kapcsolati mátrixot hozok létre a megvalósíthatóság módjai és a kockázatok csökkentésére bevezetett intézkedések között. A kutatás outputjaként bemutatom a kialakítható védett helyiség legideálisabb modelljét, amely ellenállósága megfelelőnek bizonyul a kutatás során megállapított, ismert fenyegetettségek komponenseinek. Összegzem a kapcsolódó követelményeket.

A javaslati részhez kapcsolódóan, javaslatot teszek a törvényalkotó számára, melynek során javaslom azon tevékenységek körét, melyek lehetőség szerinti megvalósításával, a gyakorlatban kapott eredmények értékelésével, műszaki tartalommal erősíthető a 90/2010. (III. 26.) kormányrendelet, 59. § megfogalmazott környezet kialakítása.

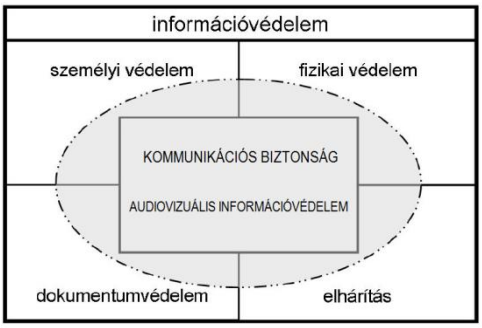
5.1 Védett helyiségek kialakítása, a védelem elemei, komplex kialakítás

Az információvédelem elméleti megközelítését vizsgálva a 3.1 fejezetben vizsgált PPT modell mellett jól alkalmazható Dr. Muha Lajos doktori disszertációjának 1. ábrája, amely a következő 39. ábrán látható.



39. ábra Az infokommunikációs biztonság és az információvédelem Forrás: [112] 20. oldal

Az 39. ábra középső halmazát „kommunikációs biztonság" és „audiovizuális információvédelem" közös halmazként elnevezve, jelen kutatáshoz illeszthető elméleti modellt kapunk a védett helyiségek audiovizuális biztonságának kialakításra, amely a 40. ábrán látható.



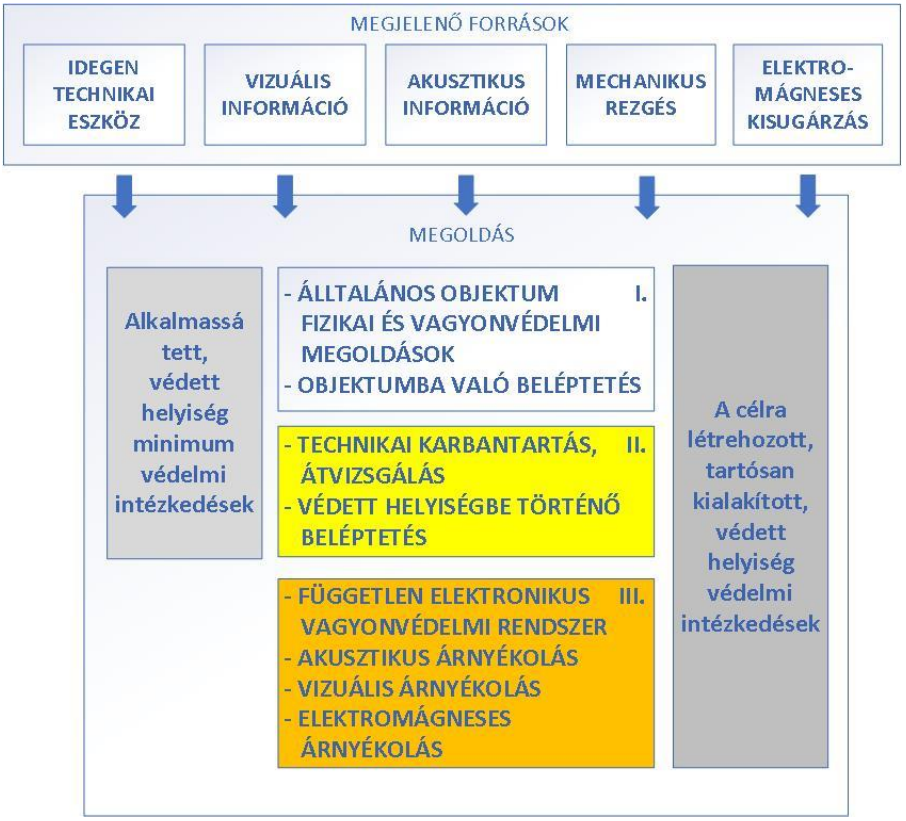
40. ábra Audiovizuális kommunikáció biztonsága és az információvédelem
Forrás [112] 20. oldal alapján saját szerkesztés

A 40. ábra személy és dokumentumvédelmi halmazait az előző részekre hivatkozva, jelen kutatás nem vizsgálja, azonban a fizikai védelem kialakítását és a mellette megjelenő újabb elemet, amely az elhárítás részhalmaz elnevezést kapta a témához illeszkedve tárgyalja.

Az elhárítás összetevő ebben az esetben ellentevékenységet, technikai karbantartást, átvizsgálást jelent. A maradványkockázat csökkentése szempontjából a védett helyiségekben és a szűkebb értelemben vett, környezetükben megjelenő fenyegetettségek feltárását, megzavarását és megszüntetését jelenti. [115] Az elhárítás halmaz esetén elsősorban nem fizikailag kialakítható valamint beépíthető eljárásról beszélhetünk, hanem humán erőforrás által végzett technikai (folyamatról) vizsgálatról, amely tudás és technikai eszközök használata révén jelentős mértékben hozzájárul a védett helyiség biztonságának kialakításához és fenntartásához.

A védett helyiségek komplex védelemének kialakítása az előző IV. fejezetben megismert támadási vektorok megismerését követően alakítható ki. A megjelenő

kockázatok forrásai beazonításra kerültek. A fenyegetettségekre hozott ellenintézkedések eredményeként, definiálhatóak az információbiztonsági kockázatok ellen létrehozható megoldások, melynek összefoglalása a 41. ábrán látható. A kockázatokra hozott **komplex** védelmi intézkedések bevezetése által válik egy objektumon belül elhelyezett őrzött helyiségből a kutatási téma szempontjából meghatározott **biztonságos „védett helyiséggé"**. A 41. ábra elemeit tételesen áttekintve, a megjelenő források mezőben a fenyegetést jelentő kockázatok láthatók.



41. ábra A védett helyiségben és az ott folytatott kommunikáció során megjelenő kockázati források és a csökkentésükre létrehozott komplex intézkedések összefoglalása Forrás: saját ábra

A halmaz elemeit áttekintve az információbiztonságot veszélyeztető idegen technikai eszköz alatt minden olyan eszközt érthetünk, amelynek funkciója ismeretlen, vagy bizonytalanságot hordoz magában az információ biztonságát illetően. A védett helyiségek üzeme során a bizonytalanságot a legkisebb mértékre kell szorítani a kockázatok csökkentése érdekében. Minden idegen, ismeretlen technikai eszköz hordozhat magában kockázatot, így azok felkutatása és kizárása fontos intézkedése a védett helyiségek üzemelésének.

A vizuális információ védett helyiségen kívüli terjedése szintén nem megengedhető, mivel az direkt értelmezhető megjelenési formában áll elő az információ értelmezése során.

Az akusztikai információ terjedése további fontos, alapvető szempont, mivel az, az emberi kommunikáció során direkt formában jelenik meg.
A mechanikai rezgés az akusztikailag előálló fizikai jelenségek további formája, amely direkt információkat hordoz a kommunikáció során megjelenő hangok hatására.
A kommunikációs környezetben használt elektronikus eszközök elektromágneses - rádiós kisugárzásai szintén a védett kommunikáció tartalmának részinformáció hordozói lehetnek, melyek elhagyhatják a kommunikációs térrészt, így információszivárgási csatornát hoznak létre.
A védett helyiségek komplex információbiztonságának kialakításához nyolc olyan átfogó védelmi célú intézkedést azonosítottam, melyek alapján három fő csoportosítást végeztem ami a 41. ábra megoldás I., II., és III. halmazait alkotják.
A védett helyiségek maradványkockázatára tett engedmények kompromisszum megoldása révén a 41. ábra I. és II. megoldás halmazának teljesítésével, többnyire ideiglenes jelleggel is kialakíthatóak. Azonban a téma szempontjából tartósan kialakítani kívánt védett helyiség létrehozása, az ábra megoldás halmazának mindegyikét kell, hogy tartalmazza a maradványkockázatok minimalizálása céljából.
A I. csoport intézkedéseinek végrehajtását követően a helyiség alkalmassá válik arra, hogy megteremthessük a téma aspektusából mérvadó ember-ember kommunikációra alkalmas védett helyiség alapját. Az I. csoport intézkedéseire épülő II. csoport intézkedései, lehetőséget biztosítanak egy alkalmassá tett – időszakos – védett helyiség kialakításához, melyben a kockázatok mértéke radikálisan csökkenthető.
Az I. és II. csoport intézkedéseire épülő III. csoport intézkedéseivel a maradvány kockázat tovább csökkenthető, a kutatás negyedik fejezetében beazonosított kockázatokkal szemben, a védett helyiség követelményeit a legátfogóbban megvalósítva. A csoportok kialakítása befolyással bír a védett helyiségben megjelenő információk fizikai információbiztonságának megteremtésére a maradványkockázat csökkentése érdekében. A következőekben ezeket sorba véve, áttekintem a védett helyiség kialakítása során bevezetett intézkedések általános tartalmát, majd részletesen bemutatom azok kialakíthatóságát.

Általános objektum fizikai és vagyonvédelmi megoldások:

Az értekezés III. fejezetében tárgyaltak szerint a védett helyiségek kialakításuk során valamilyen objektum épületrészében kerülnek kijelölésre, elhelyezésre. Az első megközelítés alapján a védett helyiségnek a fizikai és a vagyonvédelem szempontjából

megfelelőnek kell lennie. Az objektumvédelemnek a fejezetben tárgyaltak alapján, egy egészként kell kezelnie a védett objektumot, ahová csak a jogosultsággal rendelkező személyek léphetnek be, többnyire munkavégzés céljából a számukra engedélyezett területekre.

A megfelelően elhelyezett védett helyiség környezete, általános objektumvédelmi felügyelet alatt áll, melynek engedélyezett hozzáférése jól működő rendszer esetén, a védelmi intézkedést kialakító érdekkör számára naplózott eseményt generál.

Az általános objektumvédelem feladata az objektumokba való be,- és kiléptetés, a személyátvizsgálás, esetenként személyvédelemi feladatokat ellátva. [61] [68] [64] A beléptetési folyamat során személyekhez kötött jogosultságok szerint történik az objektumba való beléptetés. A személyátvizsgálások elsődleges célja a vagyonvédelem és a tiltott tárgyak elleni intézkedés, melyek többnyire vagyon elleni és személyi testi sértés elleni cselekmények megelőzését szolgálják. Az általános be és kiléptetés általában ruházat és poggyász átvizsgálást jelent. Azonban a védett helyiségek szempontjából általános megállapítás, hogy az objektumbeléptetéssel foglalkozó vagyonőri lehetőségek, csak részben képesek kiszűrni a nem kívánt technikai eszközök objektumokba való bejutását. Az általános fizikai objektum és vagyonvédelemi megoldások mégis fontos részei a védett helyiségek biztonságának, mivel a védeni kívánt helyiség környezetéhez való személyi-fizikai hozzáférést jelentősen befolyásolja. Az általános objektumvédelem megfelelő működése a védett helyiségek ellen irányuló offenzív technikai megfigyelés megvalósulásának lehetőségét nagymértékben gátolhatja, komplex megközelítése esetén a maradványkockázatot jelentősen mérsékelheti.

Az akusztikus csillapítás:

A védett helyiségek kialakítását zárt, épületszerkezetekkel határolt térben alakíthatjuk ki, ahol létrejöhet a védett, ember-ember közötti közvetlen kommunikáció. A kommunikáció egyik elsődleges információtartalmú eleme az emberi hang. A helyiségekben és annak környezetében megtalálható anyagok, az előző IV. fejezetben részletezett módon hangvezető tulajdonságokat mutatnak. A védett helyiség környezete nem terjedhet végtelen hosszúságú csillapítási távolságra, így a kísérletekből levont következtetés alapján, a védelem kialakítása a védett helyiség akusztikus csillapításának megfelelő mértékűre növelését, vagy azzal egyenértékű intézkedés kialakítását kell, hogy megvalósítsa. A csillapítás mértéke meg kell, hogy haladja a védett helyiség külső

falazata közelében tartózkodó emberi hallás határát, illetve a falazatra helyezett offenzív érzékelők szenzitivitásának mértékét. Ez meglehetősen összetett műszaki feladat, azonban a védett helyiségek ellen irányuló offenzív technikai lehetőségek mértékét véleményem szerint komplex megközelítés esetén a maradványkockázat szempontjából jelentősen mérsékelheti.

Vizuális árnyékolás:

Az ajánlott zárt kialakítással szemben azonban előfordul, hogy időszakosan alkalmassá tett védett helyiség használata során, már meglévő ablak jellegű nyílászárókkal rendelkező helyiség kerül kijelölésre. Az emberi közvetlen kommunikáció további elsődleges formája a vizuális megjelenés és elemei, melyek az előző IV. fejezetben bizonyított okok miatt védelmi kialakítást igényelnek. Véleményem szerint, komplex megközelítése esetén, a védett helyiségen kívülről történő optikai rálátás megakadályozása, jelentősen mérsékelheti a védett helyiségek ellen irányuló offenzív technikai lehetőségek mértékét a maradványkockázatot jelentősen csökkentve.

Az elektromágneses árnyékolás:

Az elektromágneses sugárzások falazaton történő áthatolását csillapító védelmi intézkedések kettős céllal rendelkeznek. A IV. fejezet kutatási eredményeit figyelembe véve, a rádiós átviteli út egy jellemző támadási vektor lehet az offenzív technikai eszközök figyelembevételével, valamint információszivárgási csatorna lehet a védett helyiségekben elhelyezett szükséges, a kommunikációt segítő elektronikus számítástechnikai és megjelenítő eszközök alkalmazása kapcsán. A kísérletek során bizonyítást nyert, hogy az elektronikus eszközök távolról detektálható, az információt hordozó jeleket bocsájthatnak ki működésük során. Ezek a jelek a védett helyiséget magába foglaló épületrésztől távolabb is detektálhatóak lehetnek. A védett helyiségben üzemelő elektronikus eszközök által létrehozott elektromágneses jelek helyiségen kívüli kisugárzásainak megakadályozása, valamint a rádiós átviteli csatorna lezárása, mágneses és rádiós szempont alapján kialakított árnyékolással megakadályozható. Az elektromágneses árnyékolás a védett helyiségek támadhatóságát és a helyiségekben üzemelő szükséges elektronikai eszközök ellen irányuló offenzív technikai lehetőségek mértékét, komplex megközelítése esetén, a maradványkockázatok szempontjából jelentősen mérsékelheti.

Független vagyonvédelmi rendszer:

A kutatás alapján kialakult szakmai álláspont alapján a védett helyiségek kialakítása kapcsán, a független vagyonvédelmi rendszer kialakítása fontos védelmi elem, mivel a védett helyiség „hermetikus" lezárása, elszeparált módon valósulhat meg az általános épület vagyonvédelmi rendszerek kialakításától. Az általános, teljes objektumokra kiterjedő vagyonvédelmi rendszerek üzeme, jelentős számú zónára, területre terjedhet ki, nagy számú technikai elem integrálásával. Továbbá a flexibilitás és variálhatóság magában hordozza a kezelésekből és az üzemzavarokból eredő hibák magasabb százalékát. A védett helyiségek vagyonvédelmi kialakítása során, nem megengedhető az irreleváns elemek téves kezeléséből vagy hibájából eredő esetleges működési zavar, így kézenfekvő annak egyértelmű, saját védelemmel való ellátása. A védett helyiségek kialakításának komplex megközelítése esetén a független vagyonvédelmi rendszer kialakítása a maradványkockázatokat jelentősen mérsékelheti.

Technikai karbantartás, átvizsgálás:

A védett helyiségek kialakításuk során, valamit azt követően technikai ellenőrzés alatt kell, hogy álljanak. A kialakítás során, meg kell bizonyosodni a kialakított környezetre kockázatot jelentő, technológiamentes homogenitásáról, valamint az idő során újból és újból igazolni szükséges a biztonság állapotának folyamatosságát és fennállását. A védett helyiség és környezete, a használata során folyamatosan változó hatásoknak lehet kitéve, melyek kockázatot jelenthetnek az üzemvitel biztonságára. Az átvizsgálás és karbantartás szakképzett, humán erőforrás felhasználásával valósulhat meg. A karbantartásnak és átvizsgálásnak a célja, a védett helyiség és környezetének átvizsgálása, a témában számításba vehető, a megjelenő információ biztonságára veszélyt jelentő technikai offenzív lehetőségek kizárása. Továbbá célja a védett helyiség, a kialakított védelmi intézkedések és a fizikai biztonság állapotának felmérése, a védett helyiség állapotának ismeretére jogosult érdekkör tájékoztatása, és a szükséges beavatkozás elvégzése.

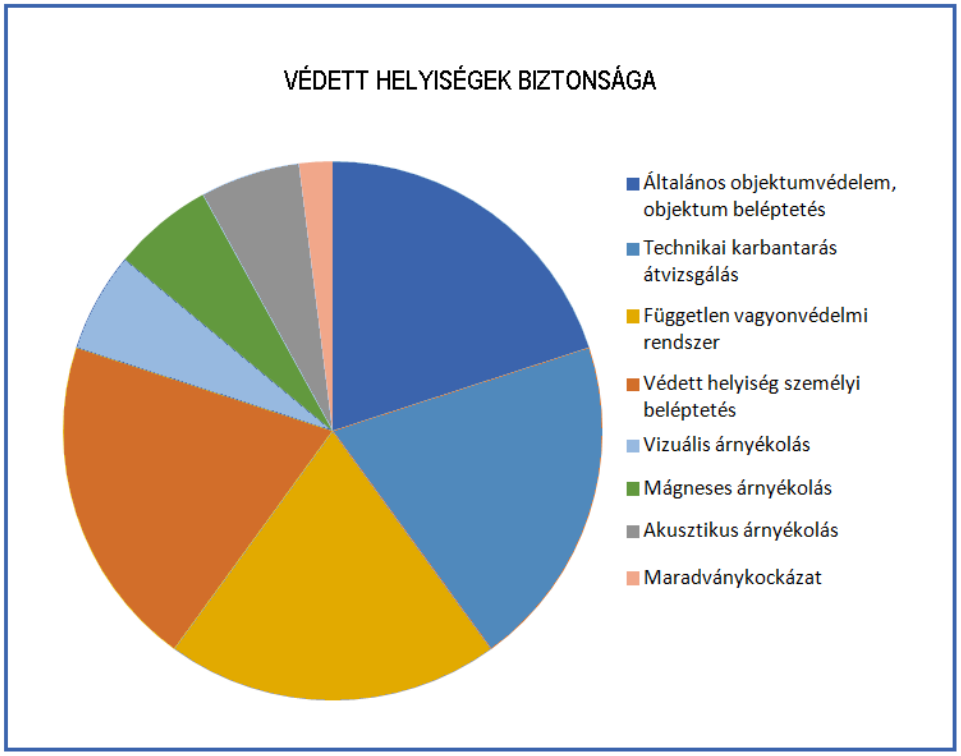
A védett helyiségek karbantartása és átvizsgálása fizikai tevékenység, amely humánerő bevonásával, technikai eszközök alkalmazásával megvalósítható munkafolyamat. A védett helyiségek kialakításának komplex megközelítése esetén a technikai karbantartás, átvizsgálás tevékenysége a maradványkockázatokat jelentősen mérsékelheti.

A védett helyiségbe történő közvetlen beléptetés:

A védett helyiségek üzemszerű használta során, a helyiségbe történő belépést megelőzően, beléptetési folyamatot célszerű beiktatni. A védett helyiségbe való beléptetés célja, az általános objektum beléptetéstől eltérően már kizárólag a védett helyiségben történő információmegosztás környezetének a védelme, az információra veszélyt jelentő offenzív technikai lehetőségek teljes kizárásával. Közvetlen a védett helyiségbe történő belépést megelőző személy és csomagátvizsgálási folyamat beiktatása jelenős kockázatcsökkentő hatást érhet el, a maradványkockázatokat jelentősen mérsékelheti.

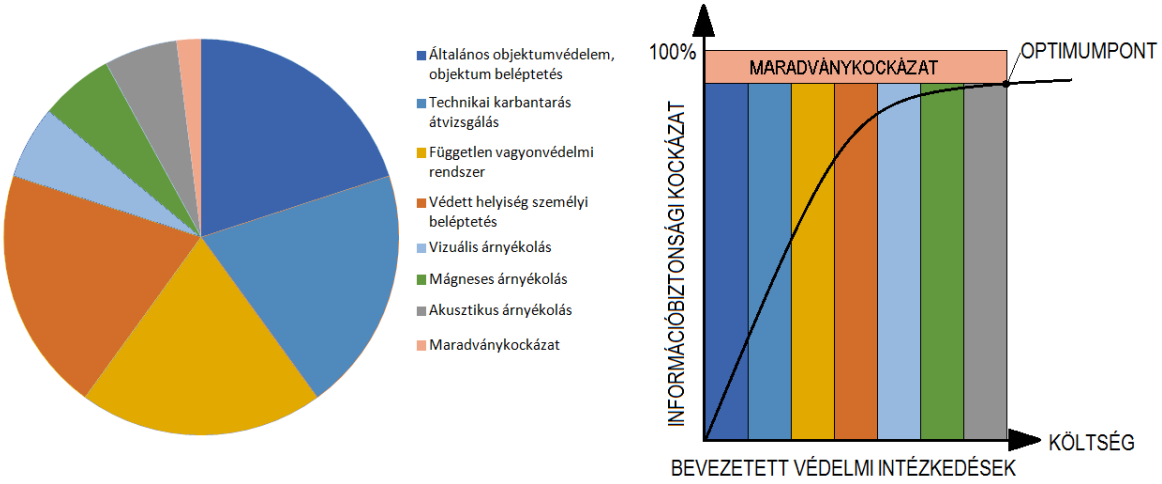
5.2 A védett helyiségek fenyegetettsége és a csökkentésükre bevezetett védelmi intézkedések kapcsolata

A védett helyiség biztonsági kockázatának csökkentésére bevezetett intézkedéseket összegezve, kördiagramon ábrázolva az alábbi 42. ábrán tekinthetjük meg. Az ábrán jelölésre került a maradványkockázat összetevő is, amely összetevő mértéke a védett helyiség kialakítására tett intézkedések megvalósításával, a leírtak alapján csökkenthető.



42. ábra Védett helyiségek fizikai biztonságának összetevői a maradványkockázat ábrázolásával
Forrás: saját ábra

Amennyiben a bevezetett védelemi intézkedések kialakításának összetevőit növeljük, a maradványkockázat értéke csökken. Másképpen ábrázolva, amennyiben a II. fejezet 3. ábráját tekintjük alapul, akkor a védelmi beruházásokat a „bevezetett védelmi intézkedések" elnevezésű tengely mentén változtatjuk, akkor az optimum pont az exponenciális görbén más-más értéket vesz fel és az intézkedések számától függően növeli vagy csökkenti a maradványkockázat értékét. Ennek ábrázolását a következő 43. ábrán szemléltetem. Az ábra megszerkesztése során - a bevezetett védelmi intézkedések azonos mértéke, és - az exponenciális görbe torzítása a szemléletes megjelenítést szolgálja.



43. ábra A védett helyiség kialakításának összetevői és az optimum pont változása a kockázatok függvényében. Forrás: saját ábra

A védelmi intézkedések kialakítása, egymásra épülő elemekből áll, melyeket meghatározott sorrendben célszerű kialakítani. Továbbá kijelenthető, hogy a bevezetett védelmi intézkedések sorrendje, nem ekvivalens értékű. A kutatás II. fejezetében tárgyaltak alapján a defenzív intézkedések és az offenzív fenyegetettség költsége egymással arányos értéket kell, hogy képviseljen, így a - bevezetett védelmi intézkedések- mértéke a megvédeni és a megszerezni kívánt információ értékével és a maradványkockázat vállalásával skálázható. [47]

A védett helyiségek kialakítása kapcsán a fenyegetettségek felmérését követően többnyire új, a hagyományosnak mondható objektumvédelemben nem használt védelmi célt szolgáló elemek bevezetése válik szükségessé, az elvi információbiztonsági rések kizárása érdekében. A következő 4. táblázat első oszlopában foglaltam össze a védett helyiségekre veszélyt jelentő források általános csoportjait (veszélyforrások). Az első

sorban feltüntetve a veszélyforrások ellen történő lehetséges védekezési formák lehetőségeivel (védelmi lehetőségek), a második sorban az intézkedés bevezetési területének megjelölésével. A táblázat további soraiban és oszlopaiban a fenyegetettségek és az ellenük alkalmazható védelmi eljárások kerültek megjelölésre, esetenként több védelmi intézkedést is jelölve, melyek összegzett hatása révén jelentősen mérsékelhetik a védett helyiség információszivárgási kockázatát az információbiztonsági kockázatot jelentő veszélyforrás feltárása és kizárása mentén.

VÉDELMI LEHETŐSÉGEK	Objektum védelem, beléptetés	Általános objektum vagyonvédelmi rendszer	Védett helyiség független vagyonvédelmi rendszer	Védett helyiségbe történő személy beléptetés átvizsgálás	Akusztikus csillapítás	Vizuális külső belátás elleni árnyékolás	Elektromágneses (mágneses és rádiós) árnyékolás	Akusztikus-rádiós zavarás	Átvizsgálás, Karbantartás, rádiós felügyelet
	A vagyonvédelem hagyományos elemeivel megvalósítható		Védett helyiség adminisztratív zónájában		A védett helyiség határoló falazatával kialakítható védelmi intézkedés			Védett helyiség környezetében	Karbantartó és műszeres ellenőrző munkálat
VESZÉLYFORRÁSOK									
Nem kívánt technológia védett helyiségbe kerülése			X	X					X
Védett helyiség külső határoló falazata felöl érkező támadás	X	X	X		X	X	X	X	X
Akusztikus megfigyelést lehetővé tevő eszközök	X	X	X	X	X			X	X
Vizuális megfigyelést lehetővé tevő eszközök	X	X	X	X		X			X
Rádiós átviteli úton működő megfigyelő érzékelők	X	X	X	X	X	X	X	X	X
Elektromágneses (mágneses és rádiós) sugárzások információtartalmából eredő biztonsági kockázatok							X	X	X
Behatolási kísérlet	X	X	X						X
A biztonság állapotának-szintjének romlása, maradványkockázat növekedése	X	X	X	X					X

4. táblázat A védett helyiségek kialakítása során feltérképezett veszélyforrások és az ellenük bevezetett védelmi intézkedések elvi lehetőségei
Forrás: saját összeállítás

A veszélyforrásokat áttekintve a védelmi lehetőségek értékelését a következő szöveges részben fejtem ki:

- Nem kívánt technológia közvetlen védett helyiségbe kerülésének kizárása kapcsán a védett helyiség független vagyonvédelmi rendszere ellenálló védelmi lehetőséget nyújt. Feltételezésem szerint a védett helyiségek nyitott állapotában, azaz az autonóm védelmi rendszer kikapcsolt állapotában folyamatos személyi felügyelet áll fenn a védett helyiség hozzáférhető részein, ami újból zárt állapotba jutásig kizárja a nyom nélküli bejutás lehetőségét. A védett helyiséget használók tekintetében a védett helyiségbe történő beléptetés külön átvizsgálással párosul, akkor csökkenthető a belépő személynél maradt kockázatos technológia védett helyiségbe való bejutásának esélye. A gyakori ellenőrzés által az átvizsgálás és karbantartás további jelentős kockázatcsökkentő hatást fejt ki mivel az idő okozta bizonytalanságot részekre osztva újra és újra zéró értékről indítja. A védett helyiség átvizsgálása és karbantartása, technikai megfelelőség esetén biztosítékot kell, hogy képezzen a védett helyiség használói számára.

- Védett helyiség külső határoló falazata felöl érkező támadás ellen szinte az összes védelmi kialakítás valamilyen gátló hatást fejt ki, mivel ez esetben a kívülről érkező technikai támadások összességével kell számolni. Az objektum védelemi és beléptetési elemei a belépési jogosultságok által korlátozzák a védett helyiség elhelyezéséül szolgáló épületbe való bejutást. A beléptetés során alkalmazható személyátvizsgálás védelmi elem csökkentheti a technológiai fenyegetettség mértékét a kockázatos eszköz megtalálásával. Az általános objektum vagyonvédelmi rendszer szintén csökkenti a védett helyiség környezetébe való eljutást, mivel a mechanikai védelem elemei gátló hatást fejtenek ki a védett épületrészekhez való hozzáférés során, továbbá dokumentált jelzést generálnak a megfelelő zónák kialakítása által a védett helyiség környezetében történt rendkívüli események érzékelésével.

  A védett helyiség független vagyonvédelmi rendszere az előzőekben leírt módon szeparált, hermetizált zónát hoz létre, a védett helyiség külső falazatának ellenőrzése által, így az általános objektumvédelem rendszereitől függetlenül, a védett helyiség sértetlenségét garantáló hatása a jogosultságok betartása és esemény jelzése és regisztrálása mentén érvényesül. A védett helyiség

akusztikus csillapítása a határoló épületszerkezeti elemek akusztikához köthető információszivárgási csatornáinak elzárását szolgálja, mivel az esetlegesen kívülről megjelenő offenzív technológia működését gátolja. A vizuális külső belátás elleni árnyékolás a külvilág felé nyílt, üvegezett nyílászárók esetén nyújt megoldást, mivel az offenzív technika feltételezett működési lehetőségét zárja ki. A védett kommunikáció során megjelenő másodlagos rádiófrekvenciás jelek védett helyiségen kívüli terjedésének az elektromágneses árnyékolás képezhet határt, amely egy a védett helyiség környezetében megjelenő, a kisugárzások vételére optimalizált technológiát használó offenzív berendezés működését lehetetleníti el, valamint a védett helyiségben ellehetetleníti a szabványos vezeték nélküli kommunikációs hálózatokhoz való hozzáférés kockázatát. Rádiós felügyelet alkalmazása esetén nagymértékben hozzájárul az eredményes frekvencia felderítés folyamatához, a védett helyiségben megjelenő kockázatot jelentő rádiós sugárforrás jelenléte gyorsan és egyértelműen kimutathatóvá válik. A zavarás, több szempont alapján is hozzájárul a védett helyiség biztonságának kialakításához, mivel a másodlagos terjedési csatornák zajjal való elárasztása a nem kívánt területeken lévő hasznos jel érzékelésének csökkenését eredményezi. Az akusztikus zavarás esetén a védett helyiség határoló felületeiben és légkapcsolatos csatornáiban kell a belülről érkező kommunikációs hangnál lényegesen nagyobb mértékű zajt generálni, így az esetleges támadóeszközök érzékelt jelein rossz jel/zaj viszonyt létrehozva, ezzel ellehetetlenítve az információ érzékelésének ezt a formáját. A rádiós zavarás többnyire a szabványos vezeték nélküli kommunikációs csatornák sávjaira korlátozódik, azonban Magyarországon ez a tevékenység nem támogatott. A passzívan kialakított (elektromágneses hullámok terjedése szempontjából árnyékolt) védett helyiség esetén, a zavarás a folyamatos rádiófelderítés és monitorozás hatásosságát a zavart csatornák tekintetében korlátozza. Megfelelően kialakított elektromágneses árnyékolás esetén a rádiófrekvenciás zavarás nem célszerű. Az érzékeny rádiómonitoring rendszer azonnali detektálást mutat az egyébként zavarási sávokban megjelenő, feltehetően tiltott eszközök jelenlétéről árulkodó csatornákban. Gyenge elektromágneses árnyékolás esetén a rádiófrekvenciás zavarás, megoldást nyújtana a szabványos, rádiókommunikációs csatornákat használó berendezések hálózathoz kapcsolódásának megakadályozására, azonban ez a törvényi szabályozók betartása miatt nem ajánlott.

Az átvizsgálás, karbantartás, rádiós felügyelet védelmi funkció az előzőek alapján a védett helyiség minőségbiztosítását alkotják, melynek során a fizikai- és műszeres vizsgálatok a védett kommunikáció időintervallumára is kiterjedhetnek, a kommunikációs környezet rádiós spektrumának megfigyelése által. Ezzel további kockázatot csökkentve a kommunikáció alatt, esetlegesen megjelenő rádiós jelek észlelése és forrásaiknak azonosítása útján.

- Akusztikus és vizuális megfigyelés ellen a védett helyiségek kapcsán az általános objektumvédelem és objektumba törtnő beléptetés elemek, valamint az általános vagyonvédelmi rendszer, védelmi hatást fejtenek ki az objektum külső határoló falazata felől érkező, látható és jelezhető támadási kísérlet azonosításával, valamint az objektumba bevinni kívánt támadóeszköz esetleges felfedésével. A védett helyiség független vagyonvédelmi rendszere a hermetikus lezárással zárhatja ki a megfigyelő eszköz védett helyiségbe történő bejutását. A védett helyiségbe történő beléptetés és átvizsgálás, szintén jelentős védelmi hatást fejthet ki az ismeretlen eszköz helyiségbe történő bejutásának megakadályozásával. Az akusztikus csillapítás, az akusztikus zavarás a védett helyiség külső falazata felől érkező audio megfigyelést lehetővé tevő technológiai támadási vektorok csökkentését szolgálja, az érzékelhetőség megakadályozása révén. A vizuális árnyékolás a védett helyiség külső falazata felől érkező vizuális megfigyelést lehetővé tevő technológiai támadási vektorok csökkentését szolgálja, az érzékelhetőség megakadályozásán keresztül. Az átvizsgálás, karbantartás ez esetben a védett helyiség biztonságos állapotát méri fel, keresi a rendellenességeket, valamint igazolja az idegen technológia mentességet és a fizikai biztonság állapotának fennállását.

- Rádiós átviteli úton működő megfigyelő érzékelő eszközök elleni védelem kialakítása során az objektumvédelem és objektumba történő beléptetés elemek, és az általános vagyonvédelmi rendszer, együttesen védelmi hatást fejthetnek ki az objektum külső határoló falazata felől, illetve a védett helyiség közvetlen külső falazata felől érkező, látható és jelezhető támadási kísérlet által, valamint az objektumba bevinni kívánt támadóeszköz esetleges előtalálása során. A védett helyiség vagyonvédelmi rendszere kizárja a megfigyelő eszköz használaton kívüli időben történő védett helyiségbe jutását. A védett helyiségbe történő

beléptetés és átvizsgálás, szintén jelentős védelmi hatást fejthet ki az ismeretlen eszköz helyiségbe történő bejutásának megakadályozásával. Ebben az esetben az akusztikus csillapítás, az akusztikus zavarás a védett helyiség külső falazata felől érkező audio megfigyelést lehetővé tevő technológiai támadási vektorok csökkentését szolgálja, az érzékelhetőség megakadályozásával. A vizuális árnyékolás a védett helyiség külső falazata felől érkező vizuális megfigyelést lehetővé tevő technológiai támadási vektorok csökkentését szolgálja, az érzékelhetőség megakadályozásával. A mágneses és rádiós árnyékolás a védett helyiségbe kerülő rádiós átvitel útján működő technológia működésének ellehetetlenítését valósítja meg. A passzív védett helyiségből a külső környezet irányába terjedő rádióhullámok csillapítása, a védett helyiség belső rádiós felügyeletének eredményességét növeli, hatékonnyá téve a megjelenő rádiófrekvenciás jelek azonnali kimutathatóságát. A rádiós zavarás többnyire a szabványos vezeték nélküli kommunikációs csatornák sávjára korlátozódik, azonban ez a tevékenység az előzőekben leírtak alapján, nem ajánlott.

Az átvizsgálás karbantartás, rádiós felügyelet védelmi funkció, a védett helyiség biztonságos állapotának felmérése, a rendellenességek kimutatása és az idegen technológia mentessége mellett a környezet rádiós felügyeletét is megteremti, folyamatos rádiós felügyeleti eszközzel a védett helyiség környezetében megjelenő rádiós jelek forrásának felderítésével.

- Mágneses és rádiós sugárzások információtartalmából eredő biztonsági kockázatok mértékének csökkentését, az előzőhöz hasonlóan a mágneses és rádiós árnyékolások által, a zavarás elvi lehetőségével, valamint az átvizsgálás karbantartás, rádiófelügyelet funkciókkal végezhetjük.

  A védett helyiségben megjelenő szükséges technikai eszközök egyedi árnyékolása, valamint a védett helyiség egészének árnyékolt kivitele, kizárhatja a kommunikáció során használt eszközök rádiós jel kibocsájtásainak helyiségen kívüli terjedését. Elvi megoldásként a rádiós jelek zavarása is az előzőekben leírtak alapján egyfajta megoldást jelenthet a problémára, azonban nem javasolt.

  Az átvizsgálás karbantartás és rádiós felügyelet funkció által azonosítható az információbiztonsági problémát hordozó berendezések köre. Ennek hatására létrehozható a kommunikációhoz szükséges berendezések köre, állandósult eszközökkel, valamint az esetlegesen kibocsájtott jelek ismerete hozzájárul a

védett helyiség biztonságos üzemeltetéséhez a védett helyiségben keletkező új jel érzékelésével, továbbá esetlegesen megjelenő új kibocsájtó eszköz kizárásával.

- A behatolási kísérlet ellen, elsődleges védelmi elemek az objektumvédelem és az általános objektum- vagyonvédelem elemei, mivel a védett helyiség elsődleges őrzési funkcióját ezen elemek határozzák meg. A következő védelmi elem a védett helyiségbe történő behatolási kísérlet ellen a védett helyiség független vagyonvédelmi rendszere, mivel a funkció telepítési céljánál fogva a védett helyiség fizikai biztonságát célzott szavatolni. A védett helyiség hermetikus lezárása a független vagyonvédelmi rendszer által valósul meg, így annak elsődleges relevanciája a behatolási kísérlet ellen egyértelmű. A behatolási kísérlet ténye, valamint annak következménye, minden esetben a védett helyiség üzemeltetésével és karbantartásával foglalkozó vizsgálatok alkalmazását vonja maga után, mivel a védett helyiség biztonsága, az esetlegesen okozott kár és a védelmi képesség felmérése, helyreállítása és szavatolása ezen funkció hatására valósulhat meg.

- A biztonság állapotának, a biztonsági szintjének romlása, a maradványkockázat növekedése, egy védett helyiség minőségi tényezője. A védett helyiség fizikai biztonságát az általános objektumvédelem, beléptetés, általános objektumvédelmi fizikai védelmi és elektronikus jelzőrendszerei alapjaiban határozzák meg. Ennek kiegészítő és a maradványkockázat mértékét csökkentő hatása a védett helyiség független vagyonvédelmi rendszere és a védett helyiség önálló beléptetési pontja. A fizikai védelmi jelző és ellenőrző elemeknek a maradványkockázat csökkentésére gyakorolt hatása, továbbá az átvizsgálás és karbantartás funkció, olyan a biztonságos állapotot igazoló kiegészítést nyújtanak, amelyek szavatolják a védett helyiség biztonságának állapotát az időnként újból és újból elvégzett vizsgálatok által. Az idő múlásával növő bizonytalansági faktort csökkentik az ellenőrző fizikai és műszeres vizsgálatok.

A védett helyiségek kutatása során a IV. fejezetében feltérképezett veszélyforrásokra és az ellentevékenységként bevezetett védelmi intézkedésekre, elvi lehetőségek alapján, a bevezetett védelmi intézkedésekkel párosítva, konkrét támadási, tevékenység-ellentevékenység párosítások állíthatóak össze (5. számú táblázat).

VÉDELMI LEHETŐSÉGEK ---------- VESZÉLYFORRÁSOK	Objektum védelem	Általános objektum vagyonvédelmi rendszer	Védett helyiség független vagyonvédelmi rendszer	Beléptetés személy átvizsgálás	Akusztikus csillapítás	Vizuális külső belátás elleni árnyékolás	Mágneses és Rádiós árnyékolás	Akusztikus-rádiós zavarás	Átvizsgálás, Karbantartás, rádiós felügyelet
vezetékes akusztikus érzékelő	X		X	X	X			X	X
vezeték nélküli elemes táplálású akusztikus rádióadó	X		X	X	X		X	X	X
vezeték nélküli elemes táplálású akusztikus rögzítő	X		X	X	X		X	X	X
hálózati táplálású akusztikus rádió adó			X	X	X				X
parabolikus akusztikus érzékelő	X					X		X	
kontakt akusztikus érzékelő	X	X						X	X
lézer akusztikus érzékelő	X					X		X	
mikrohullám táplálású akusztikus rádió adó							X	X	X
hálózati táplálású helyben működő akusztikus érzékelő			X	X					X
száloptikai kamera	X	X							X
vezetékes táplálású kamera			X			X			X
vezeték nélküli, elemes táplálású kamera rádió adó	X		X			X			X
helyben működő video rögzítő			X	X		X			X
hálózati táplálású video rádióadó			X	X		X	X		X
billentyűzet leütését figyelő eszköz			X	X			X	X	X
vezetékes telefon induktív csatoló eszköz	X	X	X	X					X
megjelenítő monitor másodlagos, kompromittáló sugárzását érzékelő detektáló eszköz	X						X		X
szabványos vezeték nélküli kommunikációs eszközök				X			X	X	X
szükséges IT eszközök					X	X	X	X	X

5. táblázat: Védett helyiségek támadási felületei, valamint az ellenük bevezetett ellentevékenységek párosítása
Forrás: saját összeállítás

5.3 Védett helyiségek kialakíthatóságának általános lehetőségei

A védett helyiségek kialakításának szokásait figyelembe véve, további értékelést jelenítek meg táblázatos formában saját elképzelésem alapján. Az értékelés a 6. számú táblázatban látható , amely a védett helyiség felmerülő kockázati elem - kockázati elem ellenintézkedés - és a védett helyiség kialakításának épített környezeti jellemzőit vizsgálja az ellenintézkedés kialakíthatóságának szempontjából.

Felmerülő kockázati elem	A felmerülő kockázat ellen hozható intézkedés	A védett helyiség kialakítása szempontjából létrehozható védelmi intézkedések a különböző védett helyiségtípusok kialakítási lehetőségeinek függvényében										
		Nem körüljárható, idegen kezelésben lévő szomszédos objektumrészekkel határolt helyiség (pl.:bérelt)			Nem körüljárható, fizikailag kívülről megközelíthetetlen, saját kezelésben lévő helyiség (pl.:föld alatt)			Körüljárható, saját kezelésben lévő szomszédos objektumrészekkel határolt helyiség			Héj szerkezetű, saját helyiségben létrehozott saját helyiség	
		LEHETSÉGES	KORLÁTOLT	NEM LEHETSÉGES	LEHETSÉGES	KORLÁTOLT	NEM LEHETSÉGES	LEHETSÉGES	KORLÁTOLT	NEM LEHETSÉGES	LEHETSÉGES	NEM LEHETSÉGES
Idegen technikai eszköz megjelenése a védett helyiség külső határoló falainál	Idegen számára kizárható legyen a határoló falazat megközelítése			X	X				X		X	
	Védett helyiség külső környezetének fizikai átvizsgálása			X		X		X			X	
	Külső héj és objektumvédelem, hozzáférhető napló és videó tartalommal		X			X		X			X	
Idegen technikai eszköz megjelenése a védett helyiségben	Védett helyiség technikai átvizsgálás	X			X			X			X	
	Személybeléptetés, beléptető rendszer,		X		X			X			X	
	Egyéni vagyonvédelmi rendszer, jelzéssel	X			X			X			X	
	Helyiség használaton kívüli időben történő hermetikus lezárása		X		X			X			X	
Léghangok hossz és keresztirányú terjedése rezgés útján	Akusztikus csillapítás beépítése a határoló falazatban			X	X			X			X	
	Zaj keltése a határoló falazatban		X		X			X			X	
Léghangok hossz és keresztirányú terjedése nyílászárókban	Zaj keltése az ablak jellegű nyílászáró szerkezetében		X		X			X			X	
	Ablak jellegű nyílászárók elhagyása			X	X			X			X	
Gépészeti elemeken keresztül terjedő rezgések	Zaj keltése az épületgépészeti csövezésben			X	X			X			X	
	Védett helyiség gépészeti csövek nélküli kialakítása			X		X			X		X	
Légbefúvók csatornái által vezetett hanghullámok és rezgések	Technikai átvizsgálás	X			X			X			X	
	A légtechnikai csatorna zajjal való telítése			X	X			X			X	
El, és átvezető vezetékek	Szükséges számú vezetékek redukálása			X	X			X			X	
	Vezetékek technikai ellenőrzése		X		X			X			X	
	Az átmenő vezetékek kizárása			X	X			X			X	
	A szükséges elmenő vezetékek szűrővel történő ellátása			X	X			X			X	

Vizuális betekintés	Árnyékolás, takarás			X	X			X			X	
	Betekintést lehetővé tevő nyílások elhagyása			X	X			X			X	
Mágneses és rádiófrekvenciás kisugárzások	Mágneses árnyékolás			X	X			X			X	
	Rádiófrekvenciás árnyékolás			X	X			X			X	
Szabványos vezeték nélküli kommunikációs eszközök	Kommunikációs eszközök védett helyiségből történő kizárása	X			X			X			X	
	Rádiófrekvenciás árnyékolás			X	X			X			X	
	Szükség esetén technikailag fizikai és IT szempontból is ellenőrzött megfelelő kommunikációs eszközök használata	X			X			X			X	
	Kommunikációs csatornák zavarása			X	X			X			X	
Idegen rádiófrekvenciás jelek a védett helyiségben vagy annak környezetében	Folyamatos védett helyiségen belüli és külső rádiófrekvenciás monitorrendszer üzemeltetése		X		X			X			X	
	Technikai átvizsgálás	X			X			X			X	
A kiépített védett helyiség biztonsági állapotának csökkenése	Rendszeres technikai átvizsgálás	X			X			X			X	
	Meghibásodások esetén azonnali hibajavítás			X	X			X			X	
	A védett helyiség használati és átvizsgálási időn kívüli hermetikus lezárása		X		X			X			X	
Ismeretlen offenzív technológia	Maradvány kockázati elem	X			X			X			X	

6. táblázat Védett helyiségek kialakítási módjai és a kockázatok csökkentésére bevezetett intézkedések kapcsolata
Forrás: saját ábra

A második fejezetben tárgyaltak alapján, kifejtésre kerültek az optimális védett helyiségek kialakításának kérdései, azonban a védett helyiségek kialakítása a gyakorlatban több irány mentén lehetséges. A védeni kívánt információ előállásának helyszíne iránti igény, újabb és újabb helyszíneken kerülhet előtérbe. Ezért a kialakítás szempontjából a védeni kívánt információ előállásának helyszíne befolyásolja a védett helyiségek kialakításának lehetőségeit. Az emberi kommunikáció során megjelenő információk védelmére tett intézkedések célja, minden esetben az audiovizuális kommunikáció során létrejött, információtartalmú fizikai jelenségek meghatározott térrészen belül tartása.

A védett helyiségek kialakításukat tekintve két fő irányban jellemezhetőek. Az első irány az épített, minden felmerülő elvi biztonsági rés kiküszöbölésére felkészített környezet kialakítása. A másik irány a szükségmegoldás, amely során a védeni kívánt kommunikáció helyszíne adott formában áll rendelkezésre. Ebben az esetben a rendelkezésre álló helyiség kockázati szintjét csökkenthetjük elfogadható mértékre,

időszakos megfelelőséget kialakítva. A fő eltérés a két kialakítás között a rendelkezésre állás időintervalluma, és a maradványkockázat értéke lehet. Egy épített védett helyiség folyamatos üzemben tartása tartósan alacsony maradványkockázat mellett megvalósítható, míg az időszakos védett helyiség magasabb maradványkockázati szintje csak adott időintervallumra szavatolható. Sorra véve a védett helyiségek kialakításának elvi lehetőségeit, először a helyiség elhelyezkedésének lehetséges formáit tekintem át, melyek alapjaiban meghatározzák a biztonsági kockázatok vállalhatóságának mértékét. A 6. táblázat szöveges értékelése a következő:

- Nem körüljárható, idegen kezelésben lévő szomszédos objektumrészekkel határolt helyiség (pl.: bérelt helyiség, szomszédos helyiségeket bérlő másik szervezet) esetén jellemezhető a legnagyobb kockázat. Ebben az esetben jelentkezik a legtöbb olyan tényező, amely gátolja a felmerülő kockázat ellen hozható intézkedések kialakításának lehetőségeit.
- Nem körüljárható, fizikailag kívülről megközelíthetetlen, saját kezelésben lévő helyiség (pl.: föld alatti kialakítás) esetén kedvezőbb helyzet áll elő a védett helyiség kialakítása kapcsán, mivel a kialakítani kívánt helyiség külső megközelítése nehézkes és rendkívül bonyolult lenne. Így a hozzáférés nehézségei miatt a kockázatot jelentő külső fenyegetés megjelenésének esélye is redukálható, azonban ezzel egyidejűleg a védekezésre kialakítható eljárások száma is csökken.
- Körüljárható, saját kezelésben lévő szomszédos objektumrészekkel határolt helyiség védett helyiséggé alakítása megfelelő lehet a kialakítás kapcsán, azonban a kockázatok mérséklése során egyes védelmi elemek kialakítása korlátos lehet a maradványkockázat csökkentésének mértéke szempontjából.
- A kutatás eredménye szempontjából a legjobb eredményt a héj szerkezetű, saját helyiségben - újonnan létrehozott - védett helyiség kialakítása adja. A felsorolt, felmerülő kockázati elemek mindegyike ellen hozható ellenintézkedés, amely elvi kizárást nyújt a felmerülő biztonsági kockázatok ellen. A továbbiakban, mint a kutatás legmegfelelőbb eredménye, az ilyen kialakítás kerül az eredmény megjelölés fókuszába, így a kapcsolódó kutatási eredmények és leírások az ilyen kialakítást helyezik előtérbe.

5.4 A védett helyiségek kialakításához kapcsolódó, a hagyományos objektumvédelmi elemektől eltérő intézkedések bemutatása

A védett helyiségek kialakítására bevezetett, az információbiztonságot növelő, a maradványkockázatokat csökkentő intézkedések áttekintése, az előzőekben a 41. ábra

alapján általánosan tárgyalásra került, azonban a kutatás során részletesen megvizsgáltam azokat. A kutatásom során megfelelőnek tartott védelmi célokat szolgáló megoldásokat rendszereztem, és az elvi kialakítások egy-egy lehetséges módját, a védett helyiség kialakításához optimalizálva a következőekben bemutatom.

5.4.1 Védett helyiség határoló falazata

A védett helyiségek kialakítása kapcsán, az egyik legfontosabb minőséget befolyásoló tényező a védett helyiség falazata. Ezt a felületet a nyílászárókkal együtt, a padlót és a mennyezetet is beleértve együtt kell kezelni az egyenszilárdság szempontjából. A védett helyiség épületben kialakított fizikai helyzetétől és fizikai védhetőségétől elvonatkoztatva, a külső irányból érkező technikai támadások ellenállóságát is, és a védett helyiségben megjelenő belső irányból kifelé haladó információtartalmú jelenségek csillapításának is a falazat szab határt. A definíció szerint a védett helyiségben megjelenő információtartalmú fizikai jelenségeknek a falazat vonalában meg kell állniuk, illetve ha a technikai megoldásokat is figyelembe vesszük, akkor azok, ha tova is terjednek, az érzékelésük és értelmezhetőségük lehetőségét a lehető legkisebb mértékűre szükséges, hogy korlátozzuk. A kivitelezhetőséget és az információbiztonsági kockázatokat áttekintve a falazatnak négy fő tulajdonságot kell megvalósítania a védett helyiségek kapcsán. Első a mechanikai szilárdság és állékonyság a fizikai védelem megteremtéséhez. A második a védett helyiségben létrejövő vizuális tartalom kívülről történő elérésének megakadályozása. A harmadik az akusztikus és mechanikai rezgések útján terjedő hangok csillapítása. A negyedik az elektromágneses úton létrejövő információszivárgási csatornák elzárása.

5.4.2 A védett helyiség falazatának szilárdsága

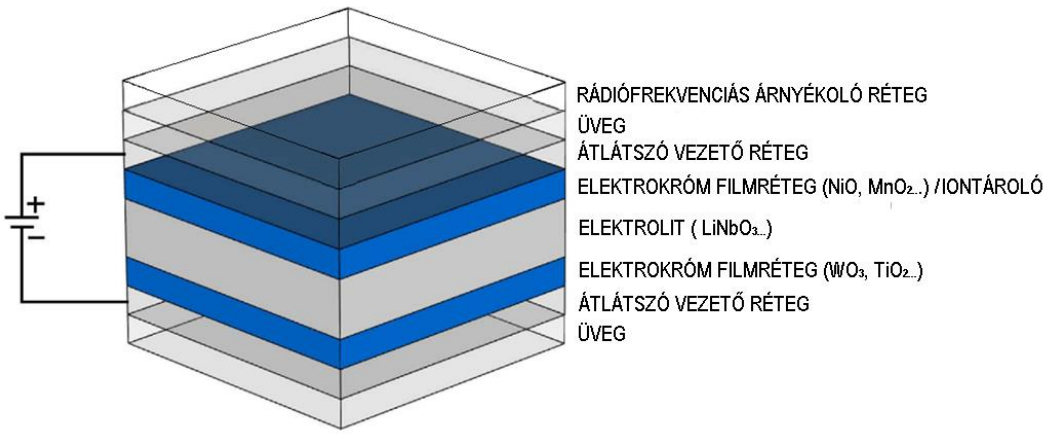
A védett helyiség falazatának megfelelően szilárdnak kell lennie. Amennyiben állami szektor esetén, a minősített adatra vonatkozó előírást is szeretnénk teljesíteni, úgy a minősített adatra vonatkozó előírásokat is implementáljuk. A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010 (III.26) Kormányrendelet 19.§ és 20.§ alapján elképzelhetőek, a kutatás tárgyául megfogalmazott védett helyiség jellemzőinek kialakításához kapcsolódó intézkedések implementálása. [36] A civil szféra esetén a Magyar Biztosítók Szövetsége általános érvényű direktíváit vehetjük alapul a vonatkozó „MECHANIKAI-FIZIKAI

VÉDELEM" fejezet „Falazatok, födémek, padozatok" pontjának megfelelően. [70]
A falazatnak a szilárdságán túl fúrás és bontásállónak kell lennie, ilyen esemény esetén azonnali riasztást kell küldenie a védett helyiségek kialakítása során egyedileg kialakított elektronikus felügyeleti berendezés útján. A védett helyiségek határoló falazatának a harmadik fejezetben leírtak alapján teljes felületvédelemmel kell rendelkeznie a külső támadások detektálhatósága érdekében, beleértve a padlót és a mennyezetet is. Az előzőekben leírtakra hivatkozva a határoló falazat további kulcsfontosságú tulajdonságának kell lennie a teljes körüljárhatósága. A védett helyiség külső épségének ellenőrizhetősége nagymértékben csökkenti a maradványkockázat értékét és elősegíti a megfelelő biztonság állapotának igazolását. A határoló falazat egyik speciális esete lehet a 6. táblázatban feltüntetett lehetőség, miszerint ha a védett helyiség alaksorban, talajjal körülhatárolt térrészben kerül elhelyezésre. Ebben az esetben a külső körüljárhatóság nem biztosítható, azonban a támadások külső kockázata is jelentősen mérséklődik a rendkívül nehéz hozzáférhetőség miatt. A határoló falazat kialakításának másik módja a védelmi elemek elosztott kialakítása. A megoldás a több rétegű, a III. fejezetben ismertetett héj szerkezetű védett helyiség térrész kialakítása, mivel így a támadási kockázatok és az azok ellen létrehozott intézkedések egyedileg hozhatók létre, az elvi kockázati tényezők egyenkénti kizárásával. A védett helyiség határoló falazatát tekintve olyan védett objektumrésznek kell tekintenünk, amely ellenáll a külső behatásoknak, biztosítja a roncsolódások tényének detektálhatóságát, valamint a talajjal körülhatárolt típus esetén részben, a többi esetben teljesen kielégíti a téma szempontjából mérvadó védett helyiség szempontjait.

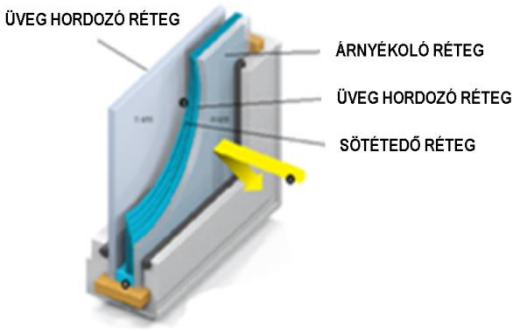
5.4.3 Védett helyiség külső belátás elleni védelme

A védett helyiségek gyakorlati kialakítása során műszaki és információbiztonsági problémát jelent a külvilág felé néző nyílászárók alkalmazása. A negyedik fejezetben bemutatott betekintési próba alkalmával gyakorlati bizonyítást nyert a nyílt üvegfelületek kapcsán jelentkező információbiztonsági probléma. Továbbá a védett helyiség falazat egyenszilárdságának kialakítását is döntő mértékben befolyásolják az ablak jellegű nyílászárok jelenléte. Az akusztikus, illetve az elektromágneses csillapítások megfelelő mértékű kialakítása komplikált megoldással érhető el az üvegfelületeken és a tokszerkezeten. Az összefüggő falazattal és a kiegészített specifikus csillapítókkal elérhető csillapítási értékek kivitelezése egyszerűbb, nagyságrenddel

meghaladja az üveggel ellátott nyílászárókon kivitelezhető csillapítások értékeit, illetve üveg jellegű felületek esetén a falazattal azonos értékű technikai megoldások kialakítása során, a nyílászáró jelentősen veszíthet a fényáteresztési jellemzőiből. A kutatás eredményeit figyelembe véve, a szempontoknak legmegfelelőbb védett helyiség kialakítása során, nem javasolom ablak jellegű nyílászárók beépítését a védeni kívánt tér határoló falazatába, mivel azok jelenléte több információbiztonsági kockázatot és technikai megvalósítási nehézséget hordoz magában. Amennyiben mégis szükséges kompromisszum elfogadása, úgy meg kell akadályozni az ablakok víztiszta átláthatóságát, léghang átvezetését és információtartalommal rendelkező rezgését, valamint ki kell alakítani a nyílászáró elektromágneses jelekkel szembeni csillapítását.
A megfelelő építészeti anyagok kutatása során, felmerült egy újszerű megoldás, a védett helyiségek üvegszerkezetének a kialakítására. A piacon található egy olyan speciális többrétegű üvegszerkezet, elektrokróm üveg (electrochromic glass), amely elektromos áram hatására elveszti átláthatóságát. A belső védett helyiség határoló szerkezetének kialakítását ily módon megvalósítva, szabályozott módon állíthatjuk annak átlátszóságát. A termék a működéséhez fémes film bevonattal rendelkezik alapvető kialakításában is nagyfrekvenciás árnyékoló hatást kifejtve. A terméket továbbfejlesztve, további rádiófrekvenciás árnyékoló réteg bevonat (RF Shielding layer) felvitelével egy olyan többrétegű üvegstruktúra lenne készíthető, amely az üveg jellegű építészeti kivitelezéshez hasonlóan, rádiófrekvenciás jelek csillapításának növelésével hozzájárul a védett helyiség árnyékolásának hatékony növeléséhez. A kialakítani kívánt üveg szerkezeti megvalósítása a 44. ábrán látható. A két üvegréteg között lévő bevonatok egyike az átláthatóságot akadályozná meg, míg a másik pedig a rádiós hullámok csillapítását végezné.



44. ábra Elektrokróm üveg eszköz tipikus felépítése Forrás: [116] alapján saját ábra



45. ábra Elektrokróm üveg nyílászáróba épített szerkezete Forrás: [117] ábra alapján

Az üveg felhasználásával véleményem szerint készíthető lenne olyan védett helyiség nyílászáró kialakítás is, amely az építészeti és fizikai követelmények túlnyomó részét kielégítené. Ennek modellje a 45. számú ábrán látható.

5.4.4 Védett helyiség határoló falazatának akusztikus csillapítása

A védett helyiségben létrejövő beszéd jellegű hangokat és kapcsolódó rezgéseket a IV. fejezetben bizonyított információbiztonsági kockázat alapján csillapítani szükséges. A védett helyiségben előálló léghangok és testhangok információtartalommal bírhatnak, és annak terjedése információszivárgási csatornaként jelentkezhet. Az építészeti akusztika tudományterületén belül hármas tagolódás különböztethető meg, amelyek a teremakusztika, a városépítési akusztika területe, valamint az épületek belső hangcsillapításának tervezését végző műszaki terület, amely az épületakusztika. Ez utóbbi a hangszigetelés tudományterülete. A védett helyiségek kialakítása kapcsán elmondható, hogy az erre a célra épített helyiségek akusztikai csillapításának kialakítása, szakosodott épületakusztikai tervező bevonását kívánja meg, mivel a falazat kialakítása az előző pontok alapján megfelelően szilárd kialakítás mellett, megfelelő akusztikai csillapítás értéket és kialakítását kell, hogy megvalósítsa. [82] [84]

A kialakítani kívánt helyiség akusztikai csillapításának tervezésekor, figyelembe kell venni a szomszédos helyiségekben elérhető érzékelési szenzitivitást, amely elsőként az emberi hallás által deklarált. Alapvetően két helyiség közötti hangcsillapítás dB-ben megadott értéke esetén, az alábbi 7. számú táblázat szemlélteti a szubjektív beszéd érthetőség, hangos zene eseteit a csillapítás függvényében, amely az átlagember hallószervéhez igazítva mutatja meg a csillapítás / áthallás viszonyát.

Két helyiség közötti hangszigetelés (dB)	Szubjektív alapon nyugvó értékelés
25dB	Normál beszéd áthallatszik
30dB	A hangos beszéd tisztán áthallatszik
35dB	A hangos beszéd egyéb zajoktól mentes esetben érthető
40dB	A hangos beszéd hallható, de nem vagy nehezen értelmezhető
45dB	A hangos beszéd alig hallható, nem értelmezhető, zene könnyen hallható
50dB	A hangos beszéd csak nagyon csendes környezet esetén hallható nem értelmezhető, zene kis mértékben hallható
65dB	Hangos zene hallható lehet, amely érzékelhető lehet hangra érzékeny szomszédos tér esetén (stúdió, koncertterem)
>70dB	A legtöbb zajt hatékonyan blokkolja

7. táblázat A beszéd érthetősége két helyiség között a csillapítás függvényében

Forrás: [118] [119] alapján

A 7. táblázatban látható, hogy a 70dB csillapítási érték közelítése lehet a mérvadó, mivel a füllel érzékelhető áthallást jó közelítéssel minden esetben kizárja. A kutatás során alkalmazható szabványosított előírásokat figyelembe véve a helyiségek közötti hangszigetelés mértékének meghatározásához jó közelítést adhat az MSZ 15601-1 szabvány. A vonatkozó részek elemzésének eredményéül a „Hangszigetelési követelmények irodaépületekben, egymás melletti helyiségek között" 4.8. táblázata alapján további értéket realizálhatunk. A tárgyalók és szomszédos helyiségek közötti hangcsillapítás értékének a szabvány alapján 54dB az alapvető fokozott léghangszigetelési követelménye, melyet a védett helyiségek rendeltetésüktől és akusztikai komfort kívánalmaiktól függően ennél magasabb csillapítási értékűre határozhatunk meg. Az MSZ 15601-1 szabvány „Léghangszigetelési követelményt növelő tényező érték" 3.1 táblázata alapján további követelmények fogalmazhatóak meg, amely alapján további 10dB-el növelhető a szomszédos helyiségek közötti léghangszigetelés értéke. A védett helyiség kialakítása során, a szomszédos épületrészek közötti léghang szigetelés kialakítása a helyiség szempontjából minőségi paraméter, amely értékének minél magasabbra történő kialakítása meghatározó a védett helyiség kapcsolódó maradványkockázata szempontjából. A kivitelezési szempontok alapján, javaslom közelíteni a 70dB akusztikai csillapítást a beszédhang tartományban. [80]

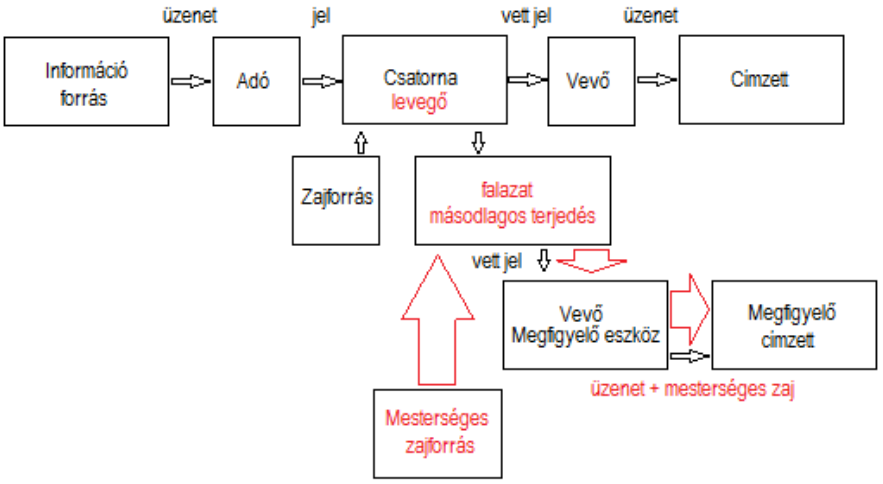
5.4.5 Védett helyiség kapcsolódó részeinek akusztikus zavarása

A IV. fejezetben végzett demonstrációs mérések alapján műszeres érzékeléssel és erősítők alkalmazásával, a védett helyiség külső falazata mentén, arra alkalmas érzékelővel, a védett helyiségben keletkező mechanikus rezgések, elektromos jellé alakítva felerősíthetőek és hallhatóvá tehetők. Ezzel hallás útján elérhető érzékelést nyújtva, információbiztonsági rést okoznak. A védett helyiségek esetén, az akusztikus csillapítás egy bizonyos mértéknél meg kell hogy álljon, ugyanis a kivitelezhetőségi szempontból a beépíthető anyagok méretének és réteges elrendezésének korlátai vannak. A határoló épületszerkezeti elemekben jelentkező információszivárgási csatorna elzárása érdekében, az információszivárgási csatorna outputja irányából vizsgálva a védelem kialakításának lehetőségét, meg kell vizsgálni a beszéd érthetőségének befolyásoló paramétereit. [120]

A fő paraméterek:

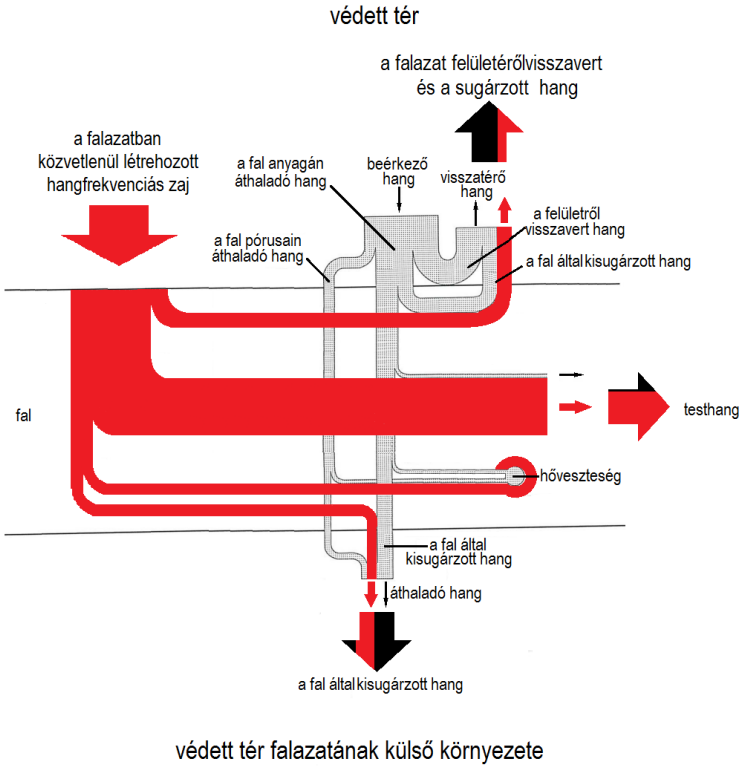
- Nyelv ismerete
- A beszélő személy artikulációs képessége
- A hallgató hallóképessége
- A direkt és zengő tér aránya, teremakusztikai paraméterek
- **Háttérzaj és hasznos jel aránya**

A nyelv ismeretén, a beszélő artikulációs képességén és az emberi hallás érzékenységén túl, alapjában véve az információbiztonság megteremtésének céljából az érzékelhető jellel arányos zaj mértékének növelését vezethetjük be, mint a cél elérésének eszközét. Ebben az esetben a feltételezett érzékelők által vett jelek hasznos jel-zaj viszonyának pozitív eltolása a cél, azaz a beszéd rezgéseire kialakult akusztikai jelek információtartalmának kívül kell esnie az értelmezhetőség határán. Gyakorlati megoldásként a helyiség határoló falait, épületgépészeti eszközeit mesterséges zajjal lehet ellenállóvá tenni, csökkentve a maradvány információbiztonsági kockázat kialakulásának feltételeit. Az épületszerkezeti és gépészeti elemekbe implementált zaj mértékének meg kell, hogy haladja a helyiségben zajló emberi kommunikációs interaktus, a helyiség elemeire gyakorolt hatását. Azaz jóval nagyobb zajt kell kelteni a határoló falak szerkezetében, épületgépészeti elemekben mint, ami a kommunikáció során fellép, amit a kommunikálók által folytatott beszédhang rezgésének erőssége okoz. A védett helyiségek akusztikus zavarásának, a IV. fejezet 10. ábrája alapján módosított elméleti modellje a 46. ábrán látható.



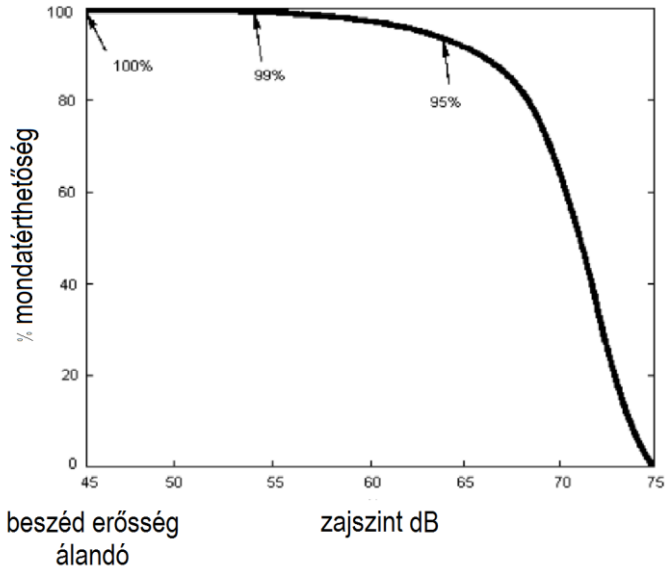
46. ábra Mesterséges zajforrással módosított Sannon - Weaver hírközlési modell
Forrás: saját szerkesztés

A falazatban terjedő és a védett téren kívül kisugárzott másodlagos rezgésekre fókuszálva a IV. fejezet 12. ábrájának módosítása alapján szemléletes ábrát kaphatunk a körülhatároló épületszerkezetekben létrehozott, zavaró hangfrekvenciás rezgéssel megrezgetett akusztikus folyamatról. A IV. fejezet 12. ábrája alapján, a zavaró rezgések energia eloszlási ábráját módosítva, a 47. ábrán látható ábrát kapjuk, amely ábrázolja a határoló épületszerkezeti és gépészeti elemekbe implementált zaj hatását.



47. ábra A védett helyiség falazatának ütköző hangenergia és a falazatba direkt módon juttatott rezgések energia megoszlása Forrás: [82] alapján saját készítésű ábra

A beszéd érthetőséget figyelembe véve az egy méternél nagyobb beszélő - hallgató távolságot feltételezve, átlag szoba méretű belső terekben 30dB alapzaj szintet feltételezve dB (SPL – Sound Pressure Level, hangnyomás szint) – 20 mikropascalra (μPa), vonatkoztatva, a beszélő által az alapzajon felül 15dB beszéd hangerőt létrehozva érhető el a megfelelő 100 százalékos beszédérthetőség. A 45dB állandó értéket fenntartva, a jel-zaj viszonyt eltolva, a zaj mértékének növelésével, az emberi hallás optimális hangnyomás határát figyelembe véve, az érthetőség negatívan befolyásolható. Ez a hatás látható a következő 48. ábrán.



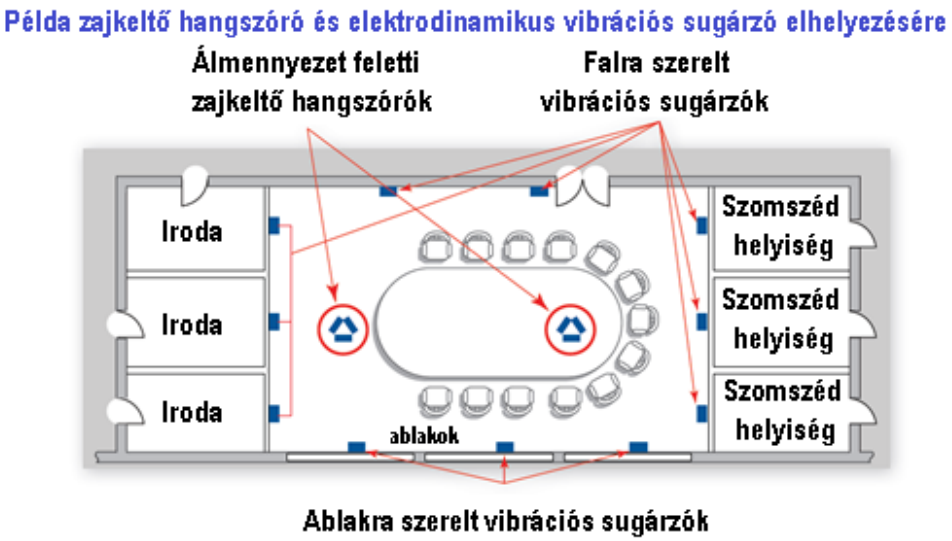
48. ábra Zajszint növekedés, mondat érthetőség diagram
Forrás: [121] (U.S. EPA, 1974b)

A szóbeli kommunikáció során a jel-zaj viszony mértéke szempontjából 15-18dB hasznos jel-zaj viszony előállása szükséges az elfogadható mondatérthetőséghez [121]. Ez az arány döntő mértékű a védett helyiségek határoló szerkezeteiben és légjárataiban, mivel a létrehozni kívánt jel-zaj arány mértéke az érzékelhető rezgésekben lévő hasznos jel értelmezhetőségét döntően befolyásolja. A határoló szerkezetekben és légjáratokban az érzékelt rezgések beszédérthetőségének javulásához nagyobb hasznos jel létrehozása lenne szükséges. A téma alapkutatása az 1950-es évekre nyúlik vissza, a Bell Telephone Laboratorie szakembereire, Harvey Fletcher és Rogers H. Galt-ra. [122]. A védett helyiségek esetén a határoló épületszerkezeti részekben és légcsatornákban létrehozott zaj, kismértékben hallható visszasugárzás által a védett térben lévők számára, így a részekben létrehozott zaj hatására, jellemzően nem emelkedik a védett térben

kommunikálók hangereje. A zaj mértéke hatással van a szótagérthetőségre, amely hatással van a mondatérthetőségre, ezáltal a hallott szöveg értelmezhetőségére. [123].

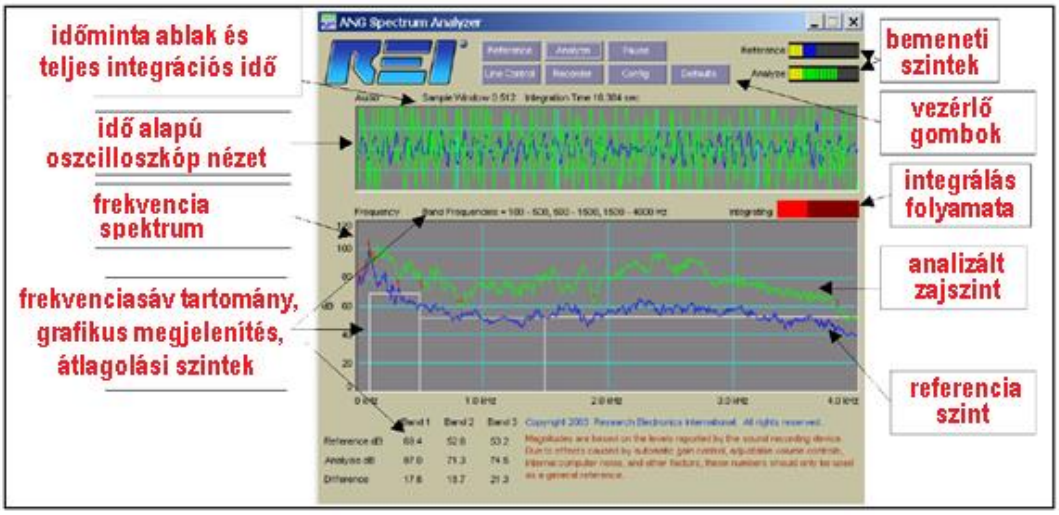
A beszéd során a magánhangzók mélyebb, míg a mássalhangzók magasabb frekvenciákat képviselnek. Az egészséges fiatal emberi hallás frekvenciasávja 20Hz-től 20 kHz-ig terjed, azonban a beszéd akusztikus energiáinak nagy része 100Hz-től 5000Hz közé esik. Az információ nagy részét ez a sáv tartalmazza. Az emberi hallás tartományát vizsgálva [124] nem lineáris érzékelésről beszélünk. A beszéd érthetőségének meghatározó jellemzője a frekvenciasáv, amely a beszédhangra jellemző. [123] A jelleggörbét megvizsgálva a 2kHz-től a 4kHz tartományban jellemzően egy érzékenyebb hallási sávról beszélünk. A beszédhang elemzése során megállapítható, hogy a védett helyiségek kapcsán alkalmazható akusztikus zavarójel spektrális jellemzőinek a 100Hz és 5kHz közötti sávban dominánsnak kell lenniük az elvi információszivárgási út elzárásának kialakításához, a beszéd hang érthetőségi jellemzőinek elnyomásával, a jel-zaj viszony megfelelő emelése céljából. A zavaró jel összetételét illetően, a fehér zaj bizonyul megfelelőnek, mivel az a teljes spektrális tartományban egyforma energiaszinttel rendelkezik. A környezeti határoló elemekben létrehozni kívánt fehérzaj előállítása során célszerű valós, félvezetőkkel előállított fehérzaj létrehozásának kialakítása, mivel a digitális ál-véletlen zaj generálása, tovább hordozza a mesterséges algoritmus által létrehozott zaj jellegű jelek elvi visszafejthetőségének kockázatát.

A védett helyiségek határoló elemeit és gépészeti eszközeit két technológiai megoldás alkalmazásával láthatjuk el zajjal. Az egyik a hangszóró jellegű készülék, mellyel a légcsatornák és üreges terek áraszthatóak el zajjal, míg a másik eszköz a testekhez mechanikusan kapcsolható „transducer" elektrodinamikus vibrációs sugárzók, melynek zaj jellegű villamos jellel rezgetett tömege szorosan kapcsolódik a védeni kívánt felülettel, határoló falazattal, abban a mozgó tömeg rezgési energiájával zajt létrehozva. A kialakítás tekintetében az alábbi 49. számú ábrán egy gyakorlati kialakítás vázlata látható, mely alapján a védett helyiség határoló épületszerkezeti elemeinek akusztikus zavarása elképzelhető. [125]



49. ábra: Védett helyiség határoló szerkezeti elemeinek és üregeinek akusztikus zavarása Forrás: [125]

A védett helyiség határoló szerkezeti elemeiben létrehozott zaj mértékét spektrálisan ábrázolva, az alábbi 50. ábrán szemléltetett módon célszerű a gyakorlatban létrehozni, ahol a beszéd spektrumát sávokra osztva a hallás tartományának különböző részein, az épületszerkezeti részeken mérhető alapzajhoz képest vizsgáljuk. Ehhez mérten keltjük az épületszerkezetben keltett zaj mértékét. A zavarás nélküli spektrumot összehasonlítva a zavarás alatt mérhető spektrummal, ábrázolható a két állapot különbsége. Így a zavarás szubjektív megítélésén túl, műszeres indikálás is ábrázolható.



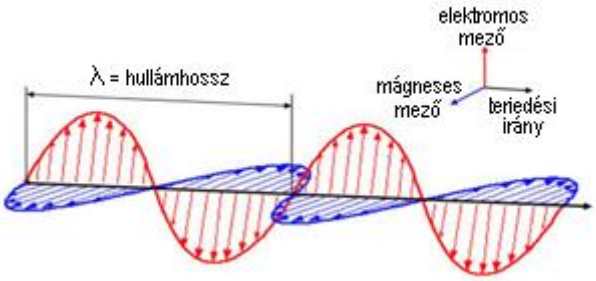
50. ábra Az épületszerkezeti részeken mérhető zavarás mértékének vizuális ábrázolása Forrás: [125]

Az elméleti forráselemzés alapján megállapított beszédérthetőség jel-zaj viszonyának értékét figyelembe véve, a határoló épületszerkezeti elemekben, valamint a védett helyiség légcsatolású gépészeti tereiben, az általános - folyamatos kommunikációs

alapzajhoz képest +20dB zaj jellegű zavaró jel létrehozása lehet célszerű a beszéd során keletkező információszivárgási csatornák lezárása érdekében.
A technológia alkalmazása esetén, a védett helyiségek kialakítása során, méréseket célszerű végezni a helyiség külső határoló falazatán, beleértve a padlót és a mennyezetet is több ponton, 2-2 méterenként alkotott rácsháló mentén, valamint a gépészeti elemeken és azok légjárataiban. A felvett mérési értékek alapján részletes kép adható a zavarás épületszerkezeti és gépészeti elemekben keltett mértékéről és a zavarás megfelelőségéről. A felvett értékeket célszerű jegyzőkönyvben rögzíteni és azt a védett helyiség karbantartása során időszakosan ellenőrizni.

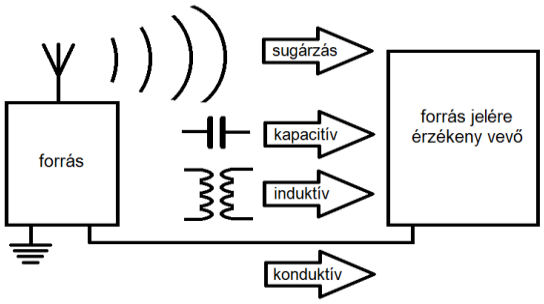
5.4.6 Védett helyiség mágneses és rádiós árnyékolása

A kutatás előző IV. fejezetében bemutatottak alapján, a védett helyiségek információbiztonságának megteremtése során, az előállás jellegétől függetlenül az elektromágneses hullámok aspektusában azok kockázatot jelenthetnek. A rádiós jellegű információ tartalmú jeleknek a védett helyiség falazatának vonalában lehetőség szerint meg kell, hogy álljanak, illetve olyan mértékűre kell, hogy csillapodjanak, hogy azok határoló falazaton túl történő érzékelésére tett kísérlet hatástalan legyen.
A védett helyiségek aspektusából kockázatot jelentő rádiós jelek keletkezésük szerint létrejöhetnek direkt módon, szabványos vezeték nélküli kommunikációs eszközből, offenzív eszköz által, valamint indirekt módon az elektronikus készülékek működéséből fakadóan. A probléma kiküszöbölésére a bevezetett védelmi intézkedések közül az elektromágneses, rádiós árnyékolás kialakítása jelent megoldást. [126] A technológia bevezetése eredményéül megakadályozható a helyiségben keletkező rádiós hullámok helyiségen kívül terjedése, valamint kialakítható a helyiség falain belül a szabványos rádiókommunikációs vezeték nélküli technológiák kizárása, azaz a helyiségen kívülről érkező, szabványos vezeték nélküli rádiós átviteli úton működő infokommunikációs eszközök hálózathoz való csatlakozásának lehetősége. A kutatás során megvizsgáltam az elektromágneses jelek keletkezését, terjedésének meghatározó formáit. A rádiós jeleket adott frekvencián rezgő elektromos jelek vezetőkben folyó áramának energiája hozza létre, elektromágneses hullám formájában. Az elektromágneses hullám az elektromos tér és a mágneses tér kombinációja, amelynek elméleti modellje a következő 51.ábrán látható



51. ábra Az elektromágneses sugárzás Forrás: [127]

A létrejött mágneses és rádiós jelek terjedése több módon is megvalósulhat: sugárzás, induktív csatolás, kapacitív csatolás és konduktív csatolás által. A terjedési módok szemléletesen az 52. ábrán láthatóak.



52. ábra: Az elektromágneses sugárzás terjedési útjai Forrás: [128] alapján saját készítésű ábra

Az elektromágneses jelek kábelszerű hullámvezetőben vonalas struktúrát követnek, míg rádióhullámként a rádiós jelek terjedésének megfelelően a térben sugározva továbbterjednek. A védett helyiségek esetén a terjedési módok kialakulásának lehetőségeit összetetten szükséges kezelni és a kialakítás tekintetében lehetőség szerint mindegyik terjedési utat le kell zárni. A nem kívánt jelterjedést árnyékolással, leválasztással és szűréssel akadályozhatjuk meg. A rádiófrekvenciás sugárzás útján terjedő hullámok terjedésének megakadályozásához árnyékolás beiktatását szükséges kialakítani, amíg a vonalas terjedés megakadályozására szűrést és leválasztást alkalmazhatunk.

A gyakorlati kialakítás tekintetében az árnyékolás megvalósítását a falazat hatékony árnyékoló anyaggal történő bevonásával érhetjük el, amelynek minőségét tekintve homogénnek, résmentesnek kell lennie.

A gyakorlatban az árnyékolt tereket Faraday-kalitkának nevezik. Az ilyen térrészbe a külső erőtér nem hatol be. A hatékonysága nagyban függ a kialakított térrész határoló szerkezetének anyagától, illetve annak ellenállásától. Rácsos szerkezet esetén a vezető szálak közötti rések meghatározzák az áthaladó jel frekvencia szerinti csillapítását.

Minél sűrűbb a rácsszerkezet, annál nagyobb rádiófrekvenciákon érhetünk el nagyobb csillapítást. A védett helyiségek esetében a kizárni kívánt rádiós frekvenciasáv a minél szélesebb rádiós spektrum. Így a minél sűrűbb rácsosztás, illetve a tömör vezető (lemez) borítás kialakítású árnyékoló szerkezet az alkalmazni kívánt megoldás.

A megvalósíthatóság szempontjából az előzőekben leírtak alapján, nem célszerű különböző ablak jellegű, nyíló felületeket létrehozni, mivel azok tartós technikai kialakítása komplikált műszaki feladat. Kivételt képeznek a bejárati nyílászáró és a légcserét szolgáló gépészeti alkalmazások nyílásai, melyek a szükséges kialakítás tekintetében nélkülözhetetlen elemei az árnyékolt védett helyiség kialakításának.

Az elektromágneses jel elektromos és mágneses összetevőinek árnyékolására, különböző anyagok mutatnak hatékony megoldást. A mágneses komponens árnyékolására a magas permeabilitású anyagok használhatóak hatékonyan, mivel azok a mágneses teret magukba zárják, így csillapítva a jelek áthatolását. A rádiófrekvenciás árnyékolás kialakítására a magasabb frekvenciákon, a 10kHz feletti sávban, a jó vezető anyagból készült borítás jelent hatékony megoldást. Ezek anyaga réz, alumínium, horganyzott acél, sűrű szövésű vezető szövet, árnyékoló festék. Az árnyékolás kialakítása szerint lehet egyszeres árnyékolás, kettős árnyékolás, kettős elektromosan szigetelt árnyékolás, átépíthető csavarozott kivitelű vagy fix kialakítású forrasztott vagy hegesztett.

A kialakítani kívánt védett helyiség egyik lényeges minőségi szempontja tehát a helyiség rádiós jelekkel szembeni ellenállósága, a rádiós jelek falazaton keresztüli csillapodása.

A kutatás során a témához kapcsolódóan felmerült a kompromittáló sugárzás, a „TEMPEST" tevékenység fogalma, amely az elektromágneses lehallgatás ellen védett készülékek tervezésére és gyártására vonatkozó szabványokat is tartalmazza, azonban a hozzá kapcsolódó leírások, pontos adatok, nyílt forrásokból nem elérhetőek. A kutatás során abból átvett adat, valamint feldolgozott háttéranyag nem készült.

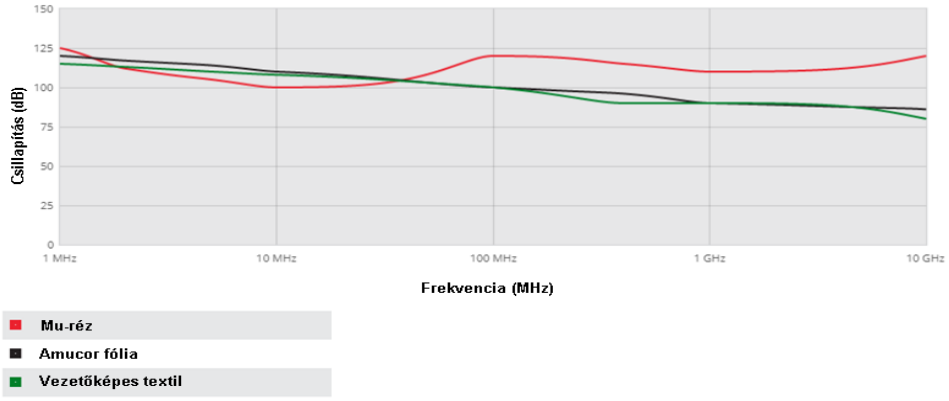
A kutatásom alapján a védett helyiségek kialakítása tekintetében az EMC (Electromagnetic Compatibility) irányelvei megfelelőek lehetnek, mivel a felmerülő rádiófrekvenciás sugárzásokból származó információbiztonsági probléma forrása a kompatibilitási problémákat okozó sugárzások forrásaival azonos problémakört képviselnek. A védett helyiségek információbiztonsága kapcsán felmerülő sugárzott, vezetett és csatolt terjedésű jelek csillapítására Magyarországon nincs elérhető előírás, azonban az EMC mérések kapcsán alkalmazott eljárások implementálása révén, a kutatás eredményéül létrehozott védett helyiség kapcsán meghatározhatóak ajánlások.

Az IEEE STD-299-2006 „Zárt terek elektromágneses árnyékolásának hatékonyság méréséhez” szabványt valamint az MSZ EN 50147-1:1998 „Visszhangmentes kamrák" minősítési szabványait megvizsgálva a védett helyiségek kapcsán ajánlhatóak mérési javaslatok. [129] [130] A szabványok tárgya az általános mérési módszerek létrehozása, a téma szempontjából árnyékolt kamrák hatékonyságának megítélésére. Az STD-299-2006 alapján alap esetben 9kHz-től 18GHz tartományban, amíg kiterjesztett esetben 50Hz-től 100GHz-ig ad mérési útmutatást. Az MSZ EN 50147-1:1998 szabvány esetén 9kHz-től 40 GHz-ig kaphatunk egységes mérési útmutatást. A hazai viszonylatokat előtérbe helyezve a védett helyiségek esetén a Magyar Szabványügyi testület által elfogadott ajánlást javaslom megvalósítani a kialakított védett helyiség árnyékolási csillapításának mérésére 9kHz-től 40GHz-ig tartományban. A védett helyiség mágneses és rádiós árnyékolásának magas értékűre történő kialakítása, ellenállóvá teszi a védett helyiség belső térrészét a szabványos rádiókommunikációs berendezések védett helyiségben történő működésével és az azok által hordozott információbiztonsági aggályokkal szemben. Nagymértékű ellenállóságot jelent a védett helyiségben direkt és indirekt módon előálló sugárzott jelek védett helyiség falazatán túljutásával szemben, az elvi információbiztonsági rés lezárása érdekében, az elvi információbiztonsági kockázat csökkentésével. A kisebb mértékű csillapítási érték kialakítása, szintén védelmet nyújthat a kisebb, a védett helyiségen belül keletkezett kisugárzások védett helyiség falazatán túljutása ellen, azonban az a szabványos rádiókommunikációs csatornákat nem zárja ki egyértelműen. Az elektromágneses csillapítás további hasznos jellemzője, hogy rádiós felügyeleti eszköz alkalmazása során, egyértelmű hatékonyságnövelő jelleggel bír a védett térrészben megjelenő nem kívánatos kisugárzások egyértelmű azonosításához.

A csillapítási érték meghatározását az alkalmas gyakorlati kivitelezés eszközeinek vizsgálatával, valamint az elérhető, témához kapcsolható szakirodalmi ajánlások figyelembevételével adhatjuk meg a kialakítani kívánt védett helyiség tekintetében.

A védett helyiségek kialakítása kapcsán alkalmazott beépített árnyékoló elemek minősége teljes mértékben meghatározza a védeni kívánt helyiség rádiós csillapításának mértékét. Az árnyékoló anyagok az előzőek alapján lehetnek fólia, textil, festék és lemez jellegűek. Egy neves gyártó termékkínálatát áttekintve a forgalmazott fólia és textil jellegű termékeinek csillapítási jelleggörbéi közül alumínium alapú fólia, réz alapú fólia, valamint a vezetőképes textil csillapítási jelleggörbéje látható az 53. ábrán. Látható, hogy termékek jelentős csillapítást érnek el az elektromágneses jelek elektromos

összetevőjének csillapítása terén.



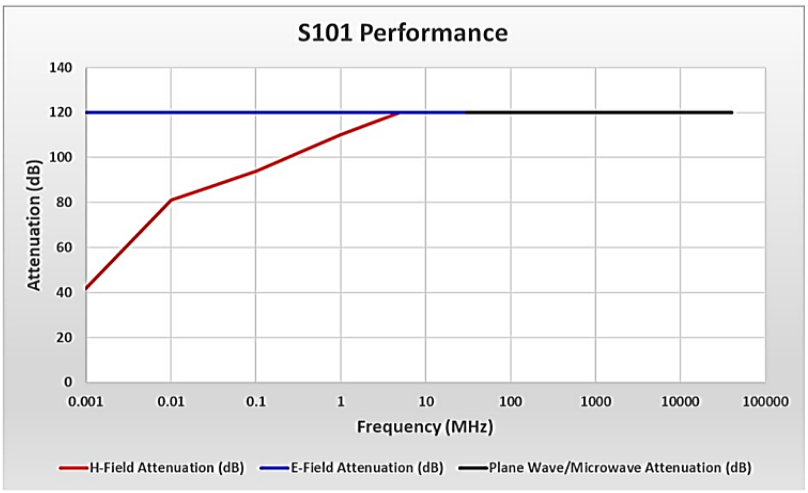
53. ábra EMC árnyékoló anyag csillapítási jelleggörbe réz alapú fólia, alumínium alapú fólia és vezető textil Forrás [131]

Ezek a termékek a helyiség árnyékolás mellett jellemzően inkább elektromos készülékek egyedi árnyékolásának kialakítására használhatóak.

Az 54. ábrán egy árnyékolt kialakítású helyiség képe látható, amely követi a különálló héj modell elrendezését. A külső határoló falszerkezeten belül került kialakításra egy árnyékoló anyagból készült merev szerkezetű helyiség, amelyben helyet kapott egy tárgyaló kialakítása.

54. ábra Faraday kialakítású helyiség Forrás: [132]

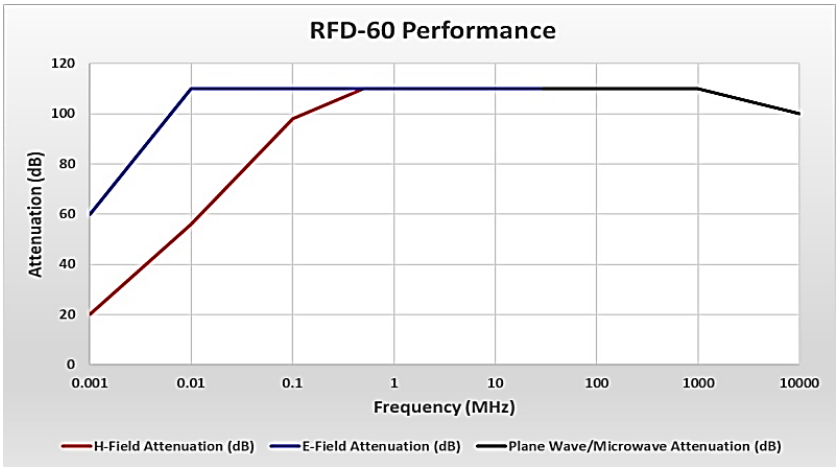
A falazat árnyékolására használható anyagokat figyelembe véve, megvizsgáltam egy lemez jellegű, árnyékoló termék jellemzőit, amely csillapítási jelleggörbéje az 55. ábrán látható.



55. ábra S101 árnyékoló panel csillapítási jelleggörbéje Forrás: [133]

Látható, hogy a termék jellemzőit tekintve külön csillapítási adattal rendelkezik a mágneses „H" field és elektromos „E" field összetevőkre vonatkozóan, valamint 50MHz feletti érték csillapítására mikrohullámú csillapítás „Microwave Attenuation" elnevezéssel. Ennek az eszköznek az esetleges használata véleményem szerint a legmagasabb igényeket is kielégíti, így a védett helyiségek kialakítása során elképzelhető alternatívát nyújthat.

Az ajtó nyílászáró kialakítása tekintetében a falazat rádiófrekvenciás árnyékoló jellemzőihez illeszkedő módon ajtó nyílászáró termék csillapítási jelleggörbéjét is megvizsgáltam, amely illeszkedik a falazathoz. Az ajtó csillapítási jelleggörbéje a következő 56. ábrán látható.

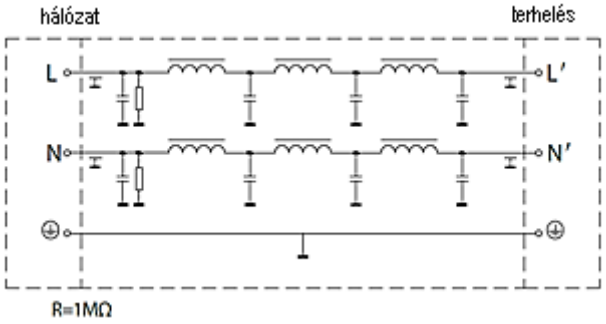


56. ábra Rádiófrekvenciás csillapító ajtó jelleggörbéje Forrás: [134]

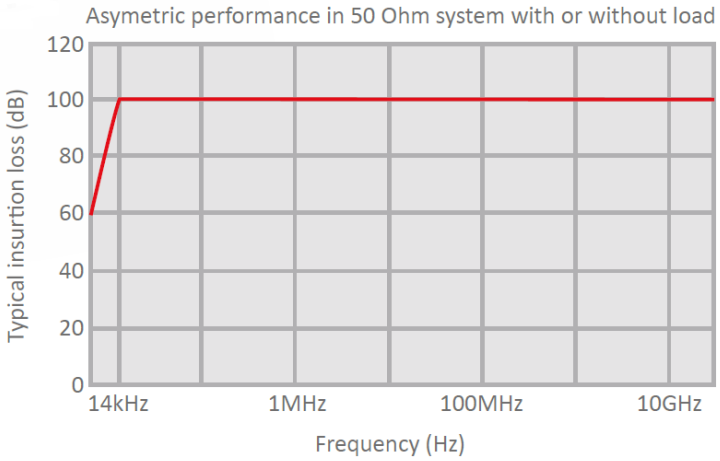
A termék jellemzőit tekintve megfelelő jellemzőkkel bír, elképzelhető alkalmazást nyújtva a védett helyiség kialakítása során.

A védett helyiségek kialakítása során további elemek az elektromos energiaátviteli

szűrők, melyek a helyiségen belül szükséges elektromos eszközök energiaellátásához használt villamos kábelek nagyfrekvenciás lezárását végzik a vezetett jelterjedés kialakulásának megakadályozása céljából. Az ilyen szűrők rendszerint áteresztő záró szűrő köröket tartalmaznak, tekintettel az átvinni kívánt jel, illetve hálózati áram frekvenciájára. Egy hálózati energiaátviteli szűrő sematikus ábrája az 57. ábrán, egy termék csillapítási jelleggörbéje pedig az 58. ábrán látható.



57. ábra Energiaátviteli szűrő kapcsolási rajza Forrás [135]

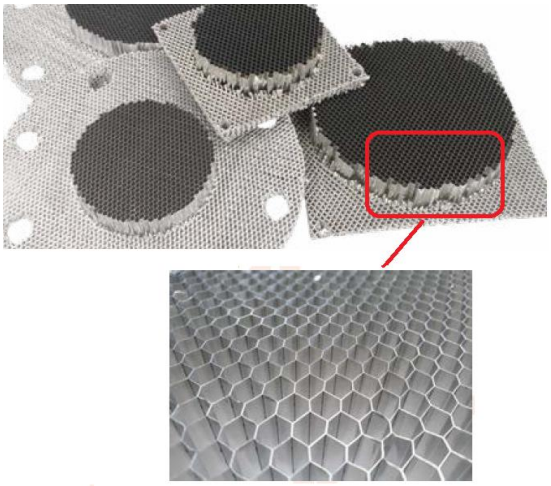


58. ábra Energiaátviteli szűrő csillapítási görbéje Forrás: [135]

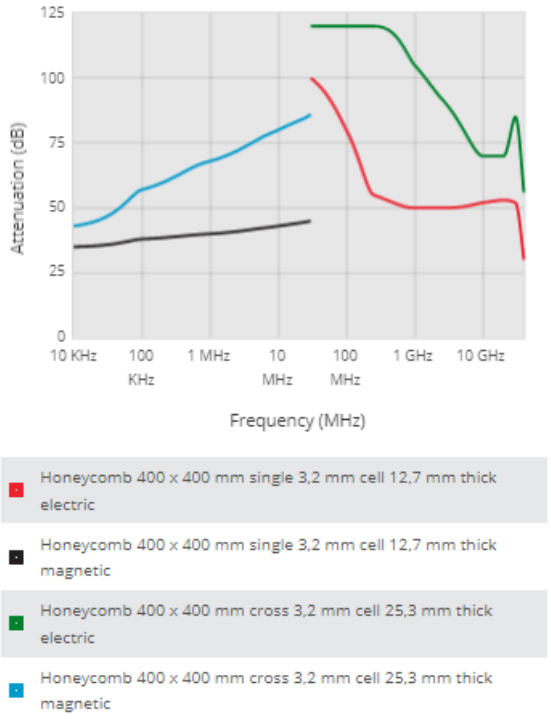
Az ábrán látható, hogy az energiaátviteli szűrő 14kHz frekvenciától 100dB névleges csillapítást nyújt. A védett helyiségek esetén az energiaátviteli szűrők további fontos feladata az energiaátviteli hálózatot, mint átviteli utat használó vezetékes offenzív technológia átviteli útjának lezárása. Ezzel ellehetetlenítve a védett helyiségből energiaátviteli hálózaton keresztüli információszivárgási csatorna kialakulását.

A védett helyiségek kialakítása tekintetében a helyiségben történő huzamos tartózkodás kialakításához nélkülözhetetlen a légcsere megvalósítása. A gyakorlatban ezt az elektromágneses csillapítás fenntartásával a gépészeti légcserélő vezetékbe épített méhsejt szerkezetű, (honeycomb) csillapító elemek beépítésével valósíthatjuk meg. A

kialakítás lényegét tekintve egy sejt szerkezetű sűrű osztású rácsnak tekinthető, amely az áthatoló levegő számára utat biztosít, viszont az elektromágneses jelek szempontjából árnyékoló hatást fejt ki. Egy ilyen szerkezeti elem képe a 59. ábrán, a csillapítási jelleggörbe a 60. ábrán látható.



59. ábra Árnyékolt szellőző átvezető szerkezete Forrás: [136]

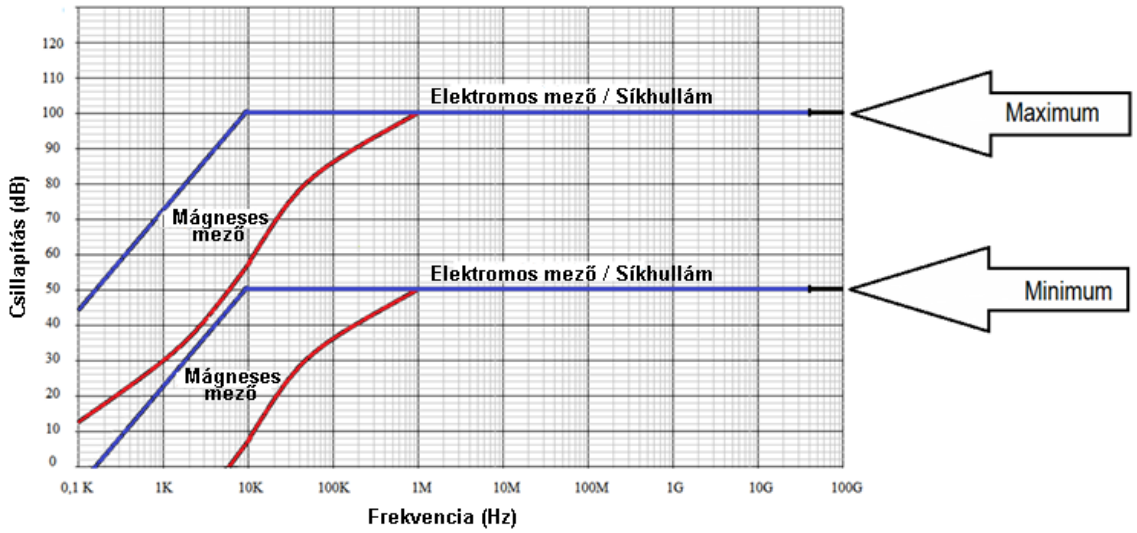


60. ábra Árnyékolt szellőző átvezető csillapítási görbéi vastagság függvényében Forrás: [136]

Az ábrán két vastagságban kialakított szűrő csillapítási görbéje látható a mágneses és elektromos tér csillapítása szerint vizsgálva. A rétegek számának növelésével ugyan a

beáramló levegő áramlási ellenállása nő, azonban a kívánt csillapítás növelhető. Így a gyakorlatban elérhető technológiai elemek csillapítási értékeit figyelembe véve, a meghatározott frekvenciasávon belül megfelelően magas értékű csillapítás kialakítható. Az elérhető írott források elemzése alapján, a Canadian Centre for Cyber Security ITSG-2 [137] útmutatása, valamint a MIL-HDBK-1195 [138] alapján a 100dB mértékű csillapítási értékek az árnyékolt helyiségek szempontjából követelményként jelennek meg, azonban a kialakítani kívánt védett helyiségek szempontjából, az elérni kívánt cél határozza meg a beépített csillapítás mértékét. Az elérni kívánt kialakítások függvényében, amennyiben a vezeték nélküli rádiókommunikációs csatornák teljes kizárás nem cél, úgy kisebb mértékű árnyékolás kialakítása is elfogadható, azonban szigorú feltételek támasztása esetén a minél magasabb csillapítási szint elérése a cél. A 61. ábrán bemutatott jelleggörbék értékei szemléltetik a tartósan kialakítani kívánt védett helyiségek általam javasolt beépített csillapítás mértékének szélső értékeit, természetesen a minél magasabb érték kialakítására törekedve.

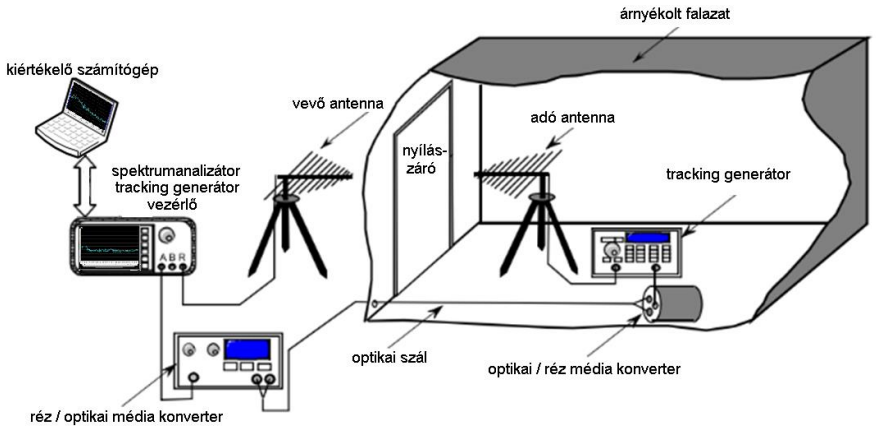
Az irodalmi források értékeit figyelembe véve, valamint a saját következtetéseket levonva a védett helyiségek kialakítása során, az árnyékolás spektrumbeli sávszélességét lehetőség szerint 9kHz-től a 40GHz-ig terjedő frekvenciasávban javaslom kialakítani és vizsgálni. [129] [130] [137] [138] [139]



61. ábra Védett helyiség csillapításának értékei a szélsőséges értékek ábrázolásával Forrás: saját ábra

Az árnyékolás csillapításának sematikus mérési elrendezését a 62. számú ábrán láthatjuk. A mérés elvégzéséhez szükség van egy spektrumanalizátor - tracking generátor összeállításra. A műszer összeállítás folyamatos jeleket szolgáltat a helyiségben elhelyezett sugárzó antenna számára. A jelek kibocsájtásával párhuzamosan a

spektrumanalizátor a helyiségen kívül elhelyezett antennán keresztül veszi az éterben megjelenő jeleket. Hitelesített adó és vevő pár esetén – amennyiben ismerjük az adó antenna sugárzott jelszintjét – bizonyos jelszintet mérve a vevő antennán, a két jelszint különbségét képezve meghatározhatjuk a két antenna közötti csillapítás mértékét.



62. ábra Az elektromágneses szempontból árnyékolt védett helyiség határoló falazatának csillapítási mérési elrendezése Forrás [140] alapján

Az antennák falazattól való távolságát az ajánlások figyelembevételével 0,3 m-re célszerű helyezni oldalanként, több mérőpont felvétele mellett. Különös figyelemmel a nyílászárók és légátvezetők nyílásai mentén, melyek vizsgálata a kifújási pontok megtalálására irányul. Az adó és vevő műszerek összeköttetését hatékonyan optikai szál segítségével valósíthatjuk meg. A vizsgálatot célszerű sávokra osztani és adott sávokon belül megfelelő nyereségű, szélessávú antennákkal elvégezni.

5.4.7 Védett helyiség szabványos vezeték nélküli kommunikációs csatornáinak rádiós zavarása

A források elemzése és a megoldások keresése kapcsán felmerült, hogy a védett helyiségek kialakítása valamit üzemeltetése során, a helyiségben és annak környezetében, a szabványos vezeték nélküli hírközlő, kommunikációs eszközök működésének megakadályozására, elvi megoldást nyújthat a rádiós sávot zavaró eszközök használata, amellett, hogy a mobil és IT eszközök fizikai jelenlétéből fakadó, elvi információbiztonsági aggályokat nem képesek teljes mértékben kizárni. Az ilyen eszközök képesek lehetnek mobilkommunikációs és IT eszközök rádiós hálózati működésében zavar okozására.

A zavaró eszközök alkalmazhatóságával szemben azonban több aggály merül fel, ezért használata nem javasolt. A rádió frekvenciasáv állami tulajdon, emellett szűkös

erőforrás. Magyarországon a témában az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) rendelkezik, tekintettel arra, hogy az 1.§ a) pontja szerint a törvény hatálya kiterjed valamennyi Magyarország területén végzett, vagy területére irányuló elektronikus hírközlési tevékenységre és minden olyan tevékenységre, amelynek gyakorlása során rádiófrekvenciás jel keletkezik. [141] Az Eht. 182.§ szakasza alapján a frekvenciahasználatról és felosztásról a Nemzeti Média és Hírközlési Hatóság (NMHH) rendelkezik a nemzeti frekvenciafelosztásról, valamint a frekvenciasávok felhasználási szabályairól szóló 7/2015.(XI.13) NMHH rendeletnek megfelelően. A rendelet 8,3kHz-től 3000GHz-ig felosztja a rádiófrekvenciás sávot és szabályozza annak felhasználását. [142] A rádiós jelek előállításáról a rádióberendezésekről szóló 2/2017. (I.17) NMHH rendelet rendelkezik. [143] Ennek 3. § szakasza alapján a rádióberendezéseket úgy kell kialakítani, hogy

- biztosítsák a káros zavarás elkerülése mellett a rádióspektrum eredményes és hatékony használatát
- ne okozzanak kárt az elektronikus hírközlő hálózatban vagy annak működésében
- ne használják olyan módon az elektronikus hírközlő hálózat erőforrásait, amivel a szolgáltatás minőségének elfogadhatatlan romlását idézné elő, és
- támogassák a segélyhívó szolgálatokhoz hozzáférést biztosító egyes funkciókat;

A rádiófrekvencia jogszerűtlen, engedély nélküli használat esetén az Eht. felhatalmazást ad az NMHH hatósági intézkedéséhez, még azt is lehetővé teszi, hogy a hatósági intézkedés zavartalan lefolytatásának biztosítása érdekében a rendőrség közreműködését kérje.

Az Eht. valamint kapcsolódó rendeleteinek értelmezése alapján, a rádiós sávot zavaró berendezések használata nem megfelelő (nem általánosan alkalmazható) megoldás a védett helyiségek komplex biztonságának kialakítása kapcsán. Alkalmazás esetén mind állami, mind civil szféra által létesített védett helyiségek környezetében gátolhatják a segélyhívó szolgálatokhoz való hozzáférés azonnali elérhetőségét. Továbbá zavaró berendezés használata az árnyékolt kialakítású védett helyiségben üzemelő rádiómonitoring rendszer működését a lefedett sávokban korlátozza. A szabványos vezeték nélküli kommunikációs eszközök védett helyiségben való kimutatása a megfelelő rádiómonitoring rendszer alkalmazásával elvégezhető, mivel azok bekapcsolt állapotukban, rádiójelek sugárzásával felfedhetik jelenlétüket a rádiómonitoring

rendszer számára. Ezért a rádiózavaró eszközök lehetséges alkalmazási módjait az árnyékolt védett helyiség kialakításának megteremtése során nem vizsgálom. A védett helyiségek üzemeltetése során a rádiós hálózati kommunikációs eszközök védett helyiségből való kizárása jelenti a teljes garanciát a rádiókommunikációs eszközök információbiztonsági kockázatainak kizárására.

5.4.8 Védett helyiségek kialakítása során alkalmazható adatátviteli csatorna kialakítása, tekintettel a monitorozhatóság követelményére

A védett helyiség használata a gyakorlatban minimális számú technikai berendezés használata nélkül elképzelhetetlen, valamint előfordulhat engedmény, aminek kapcsán a használhatóságot szem előtt tartva, a kockázatokat értékelve szükség lehet IT hálózati végpont használatára. Ebben az esetben a védett helyiség falai között ideiglenesen, ellenőrzött módon kialakított, csak a szükséges ideig ott tartott, fizikai rétegében ellenőrzött adatátviteli technológiából kicsatolt végpont kialakítása lehet a megfelelő megoldás.

Elképzelésem szerint a védett helyiség adminisztratív zónájában elhelyezhető egy informatikai végpont, amely lezárt csatlakozóval rendelkezésre áll és szükség esetén a védett helyiségbe vezethető. [144] [79] [145]

A témához kapcsolódóan a monitorozhatóság és a védett helyiségbe történő illeszthetőség tekintetében kutatást végeztem a használható technológiák kapcsán. A témát megalapozva az ellenőrizhetőséget szem előtt tartva áttekintem a lehetséges elektronikus, adatkommunikációs elveket, melyek fizikai rétege három fizikai jelenségre, és annak hírközlési technológiáira osztható:

- Elektromos vezetésen alapuló, vezetékes hírközlési technológia;
- Rádiós távközlés útján megvalósított, vezeték nélküli hírközlési technológia;
- Fény alapú, optikai szál útján megvalósított hírközlési technológia.

Az első kettő alkalmazása az előzőek alapján kevésbé kompatibilis a védett helyiségek kialakításával. Azonban a harmadik, a fény alapú megoldás, megfelelő adatkapcsolati alternatívát nyújthat. [76] [75] Vezetékes megoldások közül a legnagyobb átviteli sebességet és a legstabilabb üzemet az optikai távközlés útján érhetjük el a monitorozhatóság követelményeinek lehetőségével. A védett helyiségeket magukba foglaló épületek infrastruktúrái az informatikai adattovábbító alaphálózat meglétét feltételezik. Ez igaz az esetlegesen különböző helyen lévő védett helyiségek közötti

pont-pont szerű összeköttetésekre is. Az információs infrastruktúrák kialakítása kapcsán nélkülözhetetlen elem a stabil informatikai összeköttetés megvalósítása. Az átvitel sávszélessége az egyik alapparamétere egy informatikai rendszer minőségének és használhatóságának. Az üvegszálas adatátviteli technológiával kapcsolatos fejlesztések eredményeként, napjainkra általános eszközökké váltak az optikai szálon keresztüli adatkapcsolat megvalósításának lehetőségei. Jellemzőik miatt szinte teljesen kiszorították a korábban nagy távolságú összeköttetésekre használt egyéb technológiákat is. Az optikai szálakon keresztüli összeköttetés folyamatos üzeme létfontosságúvá vált a kritikus infrastruktúrák és a védett helyiségek folyamatos stabil üzeme kapcsán. Egy optikai szál paramétereinek megváltozása, meghibásodása azonnali hibahely meghatározás és beavatkozás igényét támasztja az üzemeltető irányába. Jelen részkutatásban témáját tekintve részletesen megvizsgáltam az optikai szálak paramétereinek változása során bekövetkező hibahely behatárolás elvi módszereit, az egyszerű módszerektől kezdve az Optical Time Domain Reflectometer (OTDR) műszerekkel történő vizsgálatokig. Az adatkapcsolati optikai szál, nemcsak az átviteli sávszélesség és egyszerű telepíthetősége miatt nagyszerű eszköze a vonalas távközlési csatornának, hanem a folyamatos működés jól monitorozhatósága is kedvező. Ezen tulajdonsága kapcsán, alkalmas pont-pont szerű védett összeköttetés megvalósítására, mint védett helyiségek közötti megbízható adatátviteli csatorna fizikai rétege. Szálfelügyeleti monitoring rendszer üzemeltetésével hosszirányú paraméterváltozás esetén, pontos hibahely behatárolásra van lehetőség. Az optikai szálak üzeme a telekommunikációs rendszerek megvalósítása mellett, a jelkódolás függvényében alkalmas titkosító által védett kommunikáció lebonyolítására is. Az információbiztonsági szempontból védett helyiségek kommunikációs csatornájaként jól alkalmazható fizikai réteg, mivel a kriptográfia eszközeinek használata mellett, folyamatos szálfelügyeleti rendszert üzemeltetve a pont-pont kommunikációs vonal a fizikai paramétereit tekintve ellenőrzés alá vonható. Kis és nagy távolságú összeköttetés estén is a szálfelügyelet a megfelelő módszer, amely szavatolja az átviteli csatornán keletkező üzemviteli hiba azonnali érzékelését és a hibahely behatárolását. Az optikai szálak további előnye a zavarérzéketlenség, a könnyű telepíthetőség, valamint a védett helyiségek térrészébe történő egyszerű bevezetés, a rádiós árnyékolás kialakításának legkevésbé gyengítése mentén. Ez az alkalmazás látható a 62 ábra mérési elrendezése során. Hátrányként megemlíthető, hogy csak speciális céleszközzel lehet a folytonossági kötéseket megvalósítani. Jelen kutatási rész célja, az optikai szálak soros paramétereinek

megváltozása estén jelentkező hibák kimutatásához szükséges elvi megoldások rendszerezése, valamint a szálfelügyeleti berendezések alapvető alkalmazásának áttekintése.

Az optikai szál esetén OTDR (*optical time domain reflectometer) berendezésekkel biztosíthatjuk egy szakasz folyamatos felügyeletét. Az OTDR szálfelügyelet egyaránt alkalmas optikai szálak kis hajlítási sugárban történő hibahelyének kimutatására, de a lassan előálló soros vonali hiba kialakulásának előrejelzésére is használható. Mivel kialakításának és alapelvének köszönhetően folyamatosan jelezheti a monitorozott optikai szál fizikai paramétereit, az üzem fenntartása közben, egyedülálló technológiaként kínál kompromisszum megoldást a védett helyiségekhez kapcsolódó pont-pont adatkapcsolat egyik kizárólagos felügyeleti alternatívájaként. A módszer alkalmas az optikai szálat érintő esetleges szabotázs azonnali jelzésére.*

Az optikai szálak visszaszórásos csillapítás mérése:

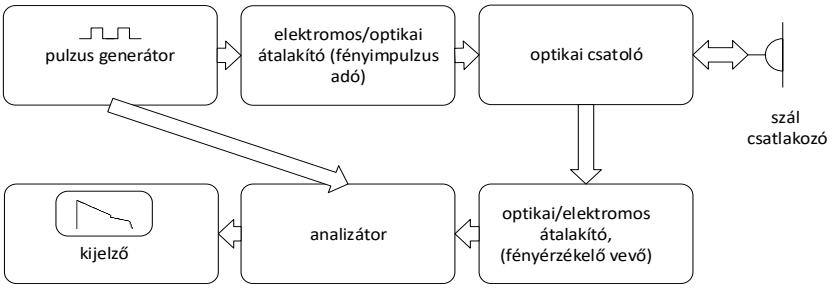
A visszaszórásos szálcsillapítás mérése jelentős előrelépést hozott az optikai szálak paramétereinek meghatározásában. A mai korszerű optikai kábelfelügyeleti rendszerek ezt a módszert használják a paraméterek, és hibák meghatározására.

A módszer alapja a Rayleigh szóráson alapul. Lényegében minden szálparaméter megváltozása esetén, a hibahelyen egy szóródás jön létre, amely szórt teljesítménye a szálban visszafelé is terjed. A visszaszórás megfelelő méréstechnikai eszközökkel érzékelhető. A védett helyiségek kontextusában egy optikai szál éles meghajlítása, elágaztatása, valamint újra toldása során, az eredetihez képest történt szálparaméter változás detektálható, így a fizikai réteg megváltozása során a változás oka kivizsgálható. A csillapítást, illetve csillapításokat, szemléletessé tehetjük az egész szál hosszán az idő függvényében. Az ilyen mérésre alkalmas műszereket OTDR-eknek (Optical Time Domain Reflectometer-nek) nevezzük. A mérés főként a következő célokra használható:

- fényvezető szálak hibahelyeinek és azok távolságainak meghatározása;
- az összekötések csatlakozási csillapításainak mérése;
- az optikai szálak fajlagos csillapításának mérésére.

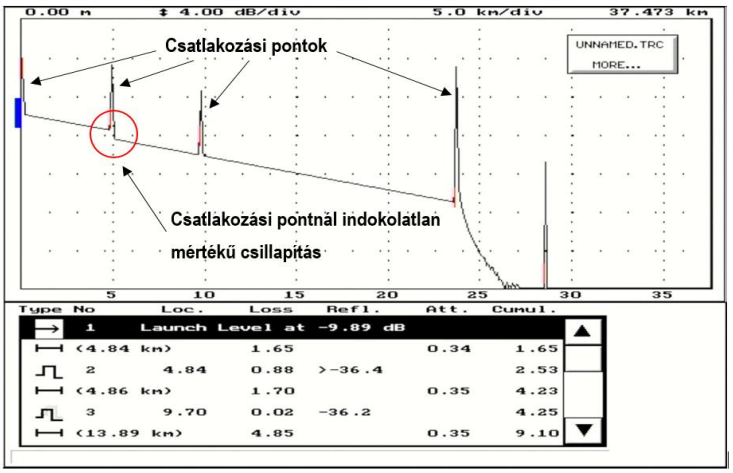
A visszaszórást monitorozva minden jelentős jellemző, amely a beüzemeléshez és az üzemeltetéshez kell, meghatározható. A mérés egy oldalról is elvégezhető jelentős előnyöket biztosítva a mérés gyors megvalósításához.

A mérés megvalósításának elve a következő: A szál bemenetére keskeny fényimpulzust vezetünk. A fényimpulzus végigterjed a szálon, miközben minden folytonossági hibáról és a szál végéről a fény egy része visszaszóródik a bemenet irányába. A szál bemenetére ahová az előző pillanatban a fényimpulzust beadtuk, egy fényérzékeny fotodiódát kapcsolunk. A visszaszóródásokból származó, a fotodióda által érzékelhetővé tett jelekből az idő függvényében ábrát készíthetünk. [146] [147] [148] Egy OTDR műszer általános elvi blokkvázlatát a 63. számú ábrán látható.



63. ábra OTDR belső felépítésének blokkvázlata
Forrás:saját rajz

Amennyiben a szál egész hosszában konstans, akkor a görbe egyenletesen csökkenő jelleget mutat. A szál végén, valamint elején ugrásszerű csúcsok jelennek meg, mert a szál törésmutatója ezeken a helyeken ugrásszerűen változik. A csatlakozási és kötési inhomogén helyeken, ahol a jellemző csillapítás eltérő az átlagostól, lépcsők láthatóak a görbén. Ezeket reflexiós helyeknek nevezzük. A kutatás során megvalósított OTDR műszer által mért gyakorlati példa képe a 64. ábrán látható. Az ábrán piros körrel jelölt esemény helyen indokolatlan mértékű csillapítás érték látható, mely egy kicsatolási pontot is takarhat.



64. ábra OTDR képernyő fotó Forrás: saját fotó

A szál hossza a fényimpulzusok szálban történő kezdet-vég-kezdet futási idejéből

határozhatóak meg A csúcsok közötti idő mérésével kiszámítható a csúcsok közötti szálhossz. A távolság, a terjedési sebesség, az időkülönbségek, és a törésmutató segítségével a következő 2. számú képlettel számítható.

$$l = \Delta t \frac{c}{n} \qquad (2)$$

Ahol

$\boldsymbol{l}$: szálhossz; **c**: 300000km/sec; **n**: törésmutató; **Δt**: csúcsok közötti törésmutató

A hossz csillapítása leolvasható a visszaszórt hossz-teljesítmény diagramból. A műszer képe a 64. számú ábrán látható.

A következő 65. ábrán egy optikai szál csillapítás mérés látható.

65. ábra OTDR mérés Forrás: saját rajz

A csillapítás értékét a 3. számú képlettel kiszámíthatjuk, ahol l_1 és l_2 a mérőszál és mért szál hosszai, valamint Pl_1 és Pl_2 a beadott és válaszként fogadott fényimpulzusok teljesítmény szintjei. [86] [149]

$$\alpha = \frac{1}{2(l_2 - l_1)} * 10log \frac{P_{l_1}}{P_{l_2}} \qquad (3)$$

A kutatás során az OTDR méréstechnika megoldásait vizsgálva szembetűnő, hogy létezik és elterjedt olyan megoldás is, amely az optikai szálak működés közbeni felügyeletét valósítja meg. [150] [151]

Ilyen megoldások a:

- Sötét szálfelügyelet WDM technológia alkalmazása esetén;
- „Out of band” sávon kívüli megoldás;
- „IN Band” sávon belüli megoldás;
- Szélessávú monitor porton keresztüli mérés.

Az optikai szálak csillapításának mérési elveit, valamint az OTDR szálfelügyeleti megoldások elméleti összefoglalóját a 2. számú melléklet tartalmazza.

5.4.9 Védett helyiség kommunikációs környezetében alkalmazott technikai berendezések, kompromisszum megoldásai

A kommunikációs környezet tekintetében beszélhetünk emberközeli az információt közvetlenül megjelenítő analóg kimenetű interfészekről, valamint a megjelenítők által

létrehozott fizikai jelenségről, amelyek információbiztonsági aggályai az értekezés előző IV. fejezetében kifejtésre kerültek. Az eredményes ember - ember közötti kommunikáció megvalósításához viszont engedményekre lehet szükség, amely technológiai kompromisszumokkal kialakítható. Konferencia berendezések tekintetében nem javasolt védett tárgyaló falai közé telepíteni azokat. Ha kompromisszumos megoldás szükséges, akkor olyan típus alkalmazása a célravezető, amelyek vezetékes kivitelűek és egységei rádiós szempontból nem generálnak kisugárzásokat. A kiegészítő alkotó elemeik elhelyezése a védett helyiség falai között, illetve az adminisztratív zónában képzelhető el. Külső stúdió alkalmazása nem javasolt. Amennyiben tolmácsberendezés szükséges, javasolt annak is a védett helyiség falai között, illetve az adminisztratív zónában tartása. Nagy helyiségek esetén, infra átviteli rendszerű tolmácsberendezés alkalmazása megfelelőnek bizonyulhat, azonban figyelemmel kell lenni az infra sugarak helyiségen belül tartására. A védett tárgyalók és a mobiltelefon technológiák használata ellentmondásos, így a mobiltelefonok okozta biztonsági rés, az esetlegesen rajtuk futó ismeretlen szoftver miatt nem tanácsos. A mobiltelefon kiküszöbölését az előzőek alapján a legegyszerűbben úgy oldhatjuk meg, hogy kitiltjuk a védett helyiség falai közül. [88] [152] [153] [154] [5] [47]

A védett helyiségekben nem ajánlott beépített videó és hang megfigyelő és rögzítő berendezés telepítése a hordozott biztonsági kockázatok miatt. Ezért szükség esetén, csak egyedileg kezelhető, rezsimintézkedésekkel kezelt rögzítő lehet megfelelő. A biztonsági rések miatt aggályos egy védett tárgyaló falai között számítógépek üzemeltetése. Azonban mivel a prezentációk kezelése megoldhatatlan számítógépek használata nélkül, elfogadható megoldás lehet olyan számítógép kialakítása, amely önálló írható-olvasható merevlemezzel nem rendelkezik. Az operációs rendszert és a prezentációs, lejátszó programot, írhatatlan módon CD lemezről futtatva működtethetjük. A szoftver tartalma a használat során nem módosul, a számítógépen a lejátszott tartalomból nem rögzülhet semmi. A számítógépnek és a kiegészítő megjelenítőknek gyengén árnyékolt védett helyiségekben lehetőség szerint árnyékolt típusúaknak kell lenniük a működésükből fakadó, kisugárzott jelek nagy távolságra terjedésének megakadályozása céljából. Amennyiben adatkapcsolati végpont kialakítása válik szükségessé, az előzőekben tárgyaltak szerint, optikai adatkapcsolati technológia felhasználásával, szálfelügyelet üzemeltetésével valósítható meg. Az IT eszköz üzemeltetése nem javasolt, azonban szükség esetén az informatikában elterjedt kriptográfiai módszerek alkalmazása révén történhet, a szükséges ideig a védett helyiség

falai között tartva. [152] [155] [156] [13] A hangsugárzók alkalmazása során törekedni kell, a normál beszéd szintjénél nem erősebb hangerő beállítására, valamit fejhallgató alkalmazása nyújthat megfelelő megoldást.

5.4.10 Védett helyiség karbantartása, technikai átvizsgálása

A védett helyiségek információbiztonsági fenyegetettségének kockázatát csökkentő intézkedések szempontjából - történő bevezetett védelmi intézkedések (41. számú ábra) és azok hatékonyságának vizsgálata kapcsán, a fenyegetettségek feltérképezése, kizárása céljából - a helyiségek átvizsgálása, valamint kialakított védett helyiségek esetén, azok karbantartása (elhárítása) jelenti az első számú védelmi intézkedést, amely a felmerülő kockázatok mértékét nagy arányban csökkenti, illetve a maradványkockázat mértékét nagyon kis értékűre csökkentheti. A védett helyiségek információbiztonsági fenyegetettségének kockázatát csak a védeni kívánt helyiség és annak környezetében lévő kockázatot jelentő paraméterek vizsgálata és értékelése után, megfelelőség megállapítását követően tekinthetjük alacsony fenyegetettségűnek.

A tevékenység végzése Magyarországon engedélyhez kötött tevékenység, amely a haditechnikai tevékenység engedélyezésének és a vállalkozások tanúsításának részletes szabályairól szóló 156/2017. (VI.16.) kormányrendelet alapján, engedéllyel rendelkező szervezetek végezhetnek. [157] Az engedély, valamint annak feltételrendszere, beszerzése nem jelen kutatás tárgya. A védett helyiségek kommunikációs célra használt környezetében, az információbiztonság felmérése és megteremtése érdekében végzett átvizsgálás és karbantartás, a helyiségek szempontjából jelentős mértékben csökkenti a maradványkockázat mértékét. Egyéni javaslatom alapján a 90/2010 (III.26.) kormányrendelet 59§.-ban meghatározott „lehallgatásmentes" környezet kialakításának alapvető kiegészítő műszaki tartalmú paraméterei lehetnének az alábbi felmérési és vizsgálati eljárások. Amennyiben a kommunikáció helyszínéül választott környezet nem az általam meghatározott védett helyiség, úgy alkalmi megoldásként, lehetőség esetén a vizsgálatok elvégzésével, és a kockázatok elemzése révén nyert megállapításokkal, a legteljesebb áttekintés adható a védett kommunikáció helyszínéül szolgáló térrész általános környezeti jellemzőiről, az információ biztonságilag alkalmas helyszín kockázatának megállapításához.

A védett, speciálisan erre a célra létrehozott helyiségek kialakításának és vizsgálatának szempontjából, és az alkalomszerűen kialakított védett térrész szempontjából a

vizsgálatok teljes körű elvégzése egyaránt átfogó érvényű tevékenység.
A javaslatom gyakorlati tartalma szempontjából az elérhető források elemzése alapján a következő eljárásokat tartalmazza. [44] [158] [159] [160] [161] [162] [17] [18]

- Alapvető információbiztonsági felmérés, amely kiterjed az:
    - Objektumvédelemre - beléptetésre;
    - Elektronikus vagyonvédelemre, jelzőrendszerre, megfigyelőrendszerre;
    - Beléptető rendszerre;
    - Fizikai védelem kialakítására;
    - Adminisztratív szabályzók, rezsimintézkedések meglétére;
    - Incidensek és azok kezelésének szabályaira;
    - Humán biztonságtudatosságra;
- Műszaki ismereteket igénylő, valamint eszközrendszeren alapuló vizsgálatok:
    - Szemrevételezés;
    - Rádióspektrum analízis;
    - Vezeték nélküli kommunikációs eszközök ellenőrzése;
    - Optikai spektrum analízis (infra tartományban);
    - Termovíziós felületanalízis;
    - Elmenő és átmenő vezetékek műszeres vizsgálata
      (vezeték felhasználására jellemző mérhető elektromos értékek: feszültségek, kábelen mérhető frekvenciák, stb.; folytonosság, azonosíthatóság, terhelések leválaszthatósága, stb.
      melyek kiterjednek: számítógépes hálózat kábelei, gépészeti vezetékek, telefon kábelek, erősáramú hálózat vezetékei, el és átmenő kábelek ellenőrzése);
    - Vezeték-kábel nyomvonal ellenőrzés;
    - Gyengeáramú végpontok, vezetékek vizsgálata;
    - Erősáramú hálózati végpontok és vezetékek vizsgálta;
    - Akusztikai szivárgás ellenőrzés (gépészeti terek, közös falak, mennyezet, padló)
    - Fizikai ellenőrzés-keresés, falazatátvizsgálás (szemrevételezés, műszeres vizsgálat)
    - Rejtett épületszerkezeti részek-üregek vizsgálata;
    - Szenzorok, elektronikus eszközök vizsgálata
- Helyszíni értékelés, -összegzés, -tájékoztatás

A védett helyiség használati idejétől, valamint a rendelkezésre állásától függetlenül az átvizsgálás, illetve meglévő védett környezet esetén, az átvizsgálás-karbantartás ad átfogó, a témában megfelelő szintű tájékoztatást a védett helyiség pillanatnyi állapotáról. Ideiglenesen kialakított, átvizsgált térrészek rendelkezési ideje, az átvizsgálást követően, a helyiség megfelelő minőségű őrzésének végéig tekinthető megfelelőnek, míg a technikai intézkedések beépítésével kialakított védett helyiség rendelkezési ideje, a beépített autonóm felügyelet, valamint specializált elrendezés által válhat tartósan megfelelőnek. A kutatás tárgya a továbbiakban a védett helyiségek vizsgálatához tartozó, közvetlen műszaki tevékenységgel kapcsolatos elérhető eszközrendszer, melynek áttekintésével a kapcsolatos feladatokról és a kivédhető technikai támadásokról kaphatunk képet. Egy a témában szakosodott gyártó termékkínálatának képe látható az alábbi az alábbi 66. ábrán.

66. ábra Védett helyiségek átvizsgálásának eszközrendszere Forrás: [99]

A kutatás során az irodalmi elemzések [44], és a témában szakosodott gyártók [99] [125] [163] [164], kínálatát áttekintve, az alábbi funkciójú berendezések alkalmazása kapcsolható a védett helyiségek átvizsgálásához, valamint karbantartásához:

- Röntgen;
- Hőkamera;
- Normál kamera;
- Endoszkóp kamera;
- Nem lineáris félvezető átmenet detektor;
- Rádiófrekvenciás spektrumanalizátor;

- Térerő indikátor;
- WIFI hálózat ellenőrző berendezések;
- Mobil hálózat ellenőrző berendezések;
- Vezeték és vonalvizsgáló berendezés;
- Nagy érzékenységű hangfrekvenciás erősítő;
- Kézi szerszámok.

Az eszközök használatához vizsgálati terület társítható, amelyekkel a feltételes kockázatok jelenléte kizárható. A vizsgáló eszközök és a hozzájuk társítható kockázatok vizsgálati területének mátrixa az alábbi 8. számú táblázatban látható.

Vizsgáló eszközök: ---------- Vizsgálati terület:	Röntgen	Hő kamera	Normál kamera	Endoszkóp kamera	Nem lineáris félvezető átmenet detektor	Rádiófrekvenciás spektrumanalizátor, térerő indikátor	WIFI-hálózat ellenőrző berendezés	Mobilhálózat ellenőrző berendezés	Vezeték és vonalvizsgáló berendezés	Nagy érzékenységű hangfrekvenciás erősítő	Kézi Szerszámok, szemrevételezés
Falazat homogenitása	X	X		X	X						X
Nehezen hozzáférhető részek vizuális vizsgálata	X		X	X	X						X
Rádiófrekvenciás közeg vizsgálata						X	X	X			
Berendezési tárgyak vizsgálata	X	X		X	X						X
Vezetékek és végpontok vizsgálata									X	X	X

8. számú táblázat Védett helyiségek technikai vizsgáló eszközei és azok vizsgálati területei
Forrás: saját ábra

Az átvizsgáláshoz, karbantartáshoz használható eszközöket, valamint feltételezett veszélyforrásokat egymás mellé állítva kimutatható, hogy a fenyegetettségek feltárásának hatásossága milyen módon érvényesülhet a vizsgálatokhoz használható technikai eszköz alkalmazásával. A IV. fejezetben feltárt fenyegetettségeket a vizsgáló eszközök vizsgálati területével összekapcsolva, valamint a tartósan kialakított védett helyiség beépített védelmi kialakításokhoz kötött eljárásokkal, egy újabb kapcsolati mátrix ábrázolható a 9. számú táblázatban, amelyen keresztül a veszélyforrások kockázata és a kockázat azonosítására és kizárására felhasználható vizsgálóeszközök és

a kockázatokat csökkentő védelmi intézkedések kapcsolata ábrázolható. A táblázatban felsorolt elemek háttérszíne a 41. ábra II. és III. halmazainak alkotói színeivel megegyező. A táblázat összeállítása során a 41. ábra I. jelű halmazának alapvető meglétét feltételezem.

	TECHNIKAI KARBANATARTÁS											KIALAKÍTOTT INTÉZKEDÉSEK				
VIZSGÁLÓ ESZKÖZÖK intézkedések ---------- VESZÉLY FOR- RÁSOK	Röntgen	Hő kamera	Normál kamera	Endoszkóp kamera	Nem lineáris félvezető átmenet detektor	Rádiófrekvenciás spektrumanalizátor, térerő indikátor	WIFI-hálózat ellenőrző berendezés	Mobilhálózat ellenőrző berendezés	Vezeték és vonalvizsgáló Berendezés	Nagy érzékenységű hangfrekvenciás erősítő	Kézi szerszámok, szemrevételezés	Beléptetés	Független elektronikus vagyonvédelmi rendszer	Akusztikus árnyékolás, zavarás	Vizuális árnyékolás	Elektromágneses rádiós árnyékolás
vezetékes akusztikus érzékelő (külön vezeték, erősáramú hálózat vezetékei)	X	X	X	X	X				X	X	X	X	X	X		
vezeték nélküli elemes táplálású akusztikus rádióadó	X	X	X	X	X	X	X	X			X		X	X		X
vezeték nélküli elemes táplálású akusztikus rögzítő	X	X	X	X	X						X		X	X		
hálózati táplálású akusztikus rádió adó	X	X	X	X	X	X	X	X			X		X	X		X
parabolikus akusztikus érzékelő														X	X	
kontakt akusztikus érzékelő													X	X		
lézer akusztikus érzékelő														X	X	
mikrohullám táplálású akusztikus rádió adó	X	X	X	X	X	X					X					X
hálózati táplálású helyben működő akusztikus érzékelő	X	X	X	X	X				X	X	X			X		
száloptikai kamera	X	X	X	X							X		X	X	X	
vezetékes táplálású kamera	X	X	X	X	X						X		X		X	
vezeték nélküli, elemes táplálású kamera rádió adó	X	X	X	X	X	X	X	X			X					X
helyben működő video rögzítő	X	X	X	X	X						X		X		X	
hálózati táplálású video rádióadó	X	X	X	X	X				X	X	X	X	X	X		X
billentyűzet leütését figyelő eszköz	X	X		X		X					X			X	X	X
vezetékes telefon lecsatoló eszköz									X	X						
megjelenítő monitor másodlagos, kompromittáló sugárzását érzékelő detektáló eszköz						X										X
szabványos vezeték nélküli kommunikációs eszközök	X	X			X	X	X	X			X	X	X	X	X	X
szükséges IT eszközök	X	X		X		X	X	X			X			X	X	X

9. számú táblázat Védett helyiségek feltételezett veszélyforrásai és az átvizsgálás során alkalmazható vizsgálóeszközök és kialakított intézkedések kapcsolata Forrás: saját ábra

A technikai karbantartás és átvizsgálás elsődleges módszere a megfigyelés, amely a szemrevételezésen alapul, majd áttevődik a technikai eszközökre és az alkalmazott műszerek érzékelési paramétereire. Az átvizsgálás a védett helyiség falazatának belső és külső tér felőli átvizsgálásával párosul. A falazat homogenitásának ellenőrzése alapvető kívánalom a védett helyiségek átvizsgálása kapcsán, amely lehetőség szerinti kockázati tényezőit a 6. számú táblázatban értékeltem. [158] [161] [162] [165]
A védett helyiségek információbiztonságára fenyegetését jelentő komponensek közül a rádiófrekvenciás kockázatokból eredő rész jelentős részt képvisel, melynek elemzése során az ilyen kockázatok kivédésére történő intézkedések alkalmazásához kapcsolódóan részkutatást végeztem.

5.4.11 A védett helyiségek rádiós környezetének vizsgálata és felügyelete

A védett helyiségek vizsgálata, kialakítása- üzemvitele során a rádiófrekvenciás környezet megismerése, valamint az ott jelenlévő-megjelenő frekvenciák eredete tisztázandó kérdéseket vet fel. A védett helyiségek környezetében található rádiós források ismerete, nélkülözhetetlen a rádiófrekvenciás fenyegetettségektől mentes állapot megállapításához, a források eredetének megismerése révén. A védett helyiségek rádiós környezetében jelen lévő jelek ellentevékenységhez kapcsolódó kérdései, két területre bonthatóak, melyek közül az egyik a rádiós jelek spektrumbeli jelenlétéhez (felderítés) és megismeréséhez kapcsolódik, míg a másik a rádiós jelek lokalizálásának módszereihez. A rádiós jelek általános megismerése spektrumvizsgálat tevékenység során lehetséges, ahol a jelenlévő jelek alapvető paraméterei (frekvencia, sávszélesség, és adott helyen mérhető térerősség) megismerhetőek. A spektrumvizsgálat során észlelt rádiós jelek jellemzőinek értékelését követően a jelek forrásának védett helyiséghez köthető kizárását javasolt elvégezni. A rádiós környezet megismerését, valamint a rádiós források azonosítását követően a védett helyiség kockázatoktól mentes üzemeltetése további rádiós felügyelet üzemeltetését teheti szükségessé. [166] [167] [168] A megjelenő rádiós jelek kimutatására alkalmazható elméleti módszerek több elv mentén is kialakíthatóak, melyek a következőek lehetnek:

- **Folyamatos rádiós sávellenőrzés elve:** melynek során a védett helyiségben egy mérőkészség kerül elhelyezésre. A műszer mérési határjellemzőitől függően, a védett helyiségben folyamatos frekvenciasáv vizsgálatot végez egy állandó

spektrumhoz képest, amely során a védett helyiségben megjelenő új rádiós jeleket érzékeli. A kutatás során áttekintett eszközök érzékelési tartományai paraméterezhetőek melyek során a védett helyiségben jelen lévő azonosított jelek engedélyezése, valamint a megjelenő ismeretlen jelekre történő riasztás megvalósítható. Az újonnan megjelenő rádiós jelek hatására azonnali jelzés generálható.

- **Azonos helyen, de eltérő időben végzett rádiós sávellenőrzés elve:** melynek során a védett helyiségben egy mérőkészség kerül elhelyezésre. A műszer mérési határjellemzőitől függően, a védett helyiségben feltérképezésre, majd azonosításra kerülnek az érzékelhető rádiófrekvenciás jelek. Ezek jellemzői rögzítésre kerülnek. Az ellenőrzés csak a releváns idősávban működik, a korábbi rögzített spektrummal való összehasonlítással. A meghatározott időben működő berendezés a védett helyiségben megjelenő rádiós jeleket érzékeli. Az azonosított jelek engedélyezése megvalósítható, így a megjelenő ismeretlen jelekre történő riasztás generálható.

- **Helyben és időben különböző, szétválasztó rádiós sávellenőrzés elve:** melynek során a védett helyiség külső környezetében egy mérőkészség kerül elhelyezésre. A műszer mérési határjellemzőitől függően, a környezetben feltérképezésre kerülnek az érzékelhető rádiófrekvenciás jelek. Ezek jellemzői rögzítésre kerülnek. A rögzítést követően, időben később, a védett helyiségben is összehasonlító rádiós spektrumvizsgálat kerülhet megvalósításra. A külső rögzített spektrumjellemzőktől pozitívan eltérő, védett helyiségen belül megjelenő rádiós jelek alapján a védett helyiségben erősebben megjelenő rádiós jelek érzékelhetőek. Az azonosított jelek engedélyezése, valamint a megjelenő ismeretlen jelekre történő riasztás generálható.

- **Azonos időben, térben szétválasztó rádió sávellenőrzés elve:** melynek során a védett helyiségben, valamint annak külső környezetében egy-egy, egymáshoz kapcsolt mérőkészség kerül elhelyezésre. A műszerek mérési határjellemzőitől függően, a védett helyiségben és annak környezetében folyamatos frekvenciasáv vizsgálat kerül elvégzésre az egymáshoz viszonyított spektrumkép összehasonlításával. A védett helyiségben elhelyezett mérőkészség a megjelenő

új rádiós jeleket érzékeli és a külső térhez képest megjelenő jelerősség alapján értékeli. A védett helyiségben újonnan megjelenő markáns rádiós jelek hatására azonnali jelzés generálható.

A védett helyiségek kialakítása során bevezetett rádiófrekvenciás árnyékolás minősége, jelentős mértékben befolyásolja a rádiófrekvenciás sávellenőrzés minőségét, valamint hatékonyságát. Egy nem, illetve gyengén árnyékolt helyiség esetén, a helyiség külső környezetében előforduló számtalan rádióforrás sugárzási energiája hatással van a védett helyiség kialakításához kapcsolható rádiós sávellenőrzés találataira, úgy egy jól árnyékolt védett helyiség falain belül működő rádiós sávellenőrző készség nagy pontosságú találati megjelenítést produkálhat a védett helyiséget érintő, nem kívánatos rádiós jelek tekintetében.
Egy, a folyamatos rádiós sávellenőrzésre használható, minimális kiépítésű műszer képe az alábbi 67. számú ábrán látható. A műszer érzékeli a közelében lévő rádiófrekvenciás jelek intenzitását, melyek küszöbérték feletti megjelenése esetén jelzést generál.

67. ábra Vezeték nélküli rádiós aktivitás ellenőrzésére szolgáló eszköz Forrás: [169]

A megjelenő rádiós jelérzékelés következményeként, a megjelenő jelzések értékelése során, a kockázatosnak értékelt rádiós jelek esetén, meg kell vizsgálni azok keletkezési forrásainak helyét. Helymeghatározásra lehet szükség, melynek során meg kell állapítani, hogy a megjelenő rádiós jel, összefüggésbe hozható-e a védett helyiség fenyegetettségének kockázatával. A kutatás részeként, a következőekben a lokalizáció eljárásait tekintem át.

5.4.12. A védett helyiség környezetében sugárzó rádió adó lokalizálásának módszerei

A rádiós környezet folyamatos vizsgálata, valamint a megjelenő új frekvenciák detektálása az előzőekben tárgyaltak szerint több módon lehetséges. A védett helyiség

környezetében megjelenő rádiós források kockázatainak felmérése érdekében a rádiós jelek forrásainak azonosítása szükséges feladat lehet. Egy rádiós sugárforrás lokalizálására a rádiós iránymérés és helymeghatározás módszerei, valamint azok kombinációi adnak lehetőséget. Felsorolva a módszereket a következő elvi lehetőségek állnak rendelkezésre:

Az AOA (Angle of Arrival) A jel beesési szöge szerinti mérése. Amennyiben egy antennát, mint irányított térbeli szűrőt alkalmazunk, egy jel sugárzási irányát több térbeli referenciapontról iránymméréssel megmérjük, akkor a metszéspontot számítással vagy ábrázolással értékelve megkapjuk a forrás helyzetét. Sűrűn épített, valamint belső terekben az árnyékolások, valamint a tükröződések (reflexiók) miatt korlátozott hatásfokkal alkalmazható. A módszer kiemelkedően az állandó jellegű jelek felderítése során hatásos [170].

Következő megoldás lehet a TDOA (Time Difference of Arrival), a jelek beérkezése közötti időkülönbség mérése, valamint a TOA (Time of Arrival), a jel beérkezés idejének mérésén alapuló módszer. A módszer alkalmazásához legalább három vételi pont egyidejű felállítása szükséges. Mivel a védett helyiségek környezetében megjelenő releváns rádiós sugárforrások teljesítménye nagy valószínűséggel kicsi, így helymeghatározás során a mérési pontok távolsága is ezzel arányosan, az érzékenység függvényében kicsi. Ebből adódóan nagy pontosságú időmérésre, valamint a vételi pontok között pontos időszinkronra van szükség. A módszer kiemelkedően az impulzus jellegű jelek felderítése során hatásos. Az eljárás szabadtéri méréseknél rendszerint jól alkalmazható, azonban épített környezetben az interferencia, valamint többszörös úton történő jelterjedés esetén nem adnak minden esetben kielégítő eredményt. Sűrűn épített környezetben és épületek belső terében a rádiós jelek felderítése során a legfőbb problémát a jelek tárgyakról való visszaverődése és azok szóródása okozza. Az épületeken belüli rádiós forrás helymeghatározására kedvezőbb megoldást nyújt a jelerősség csökkenés alapján történő beazonosítás, az RSS (Received Signal Strength) módszer. Ismerve a közeg csillapítását, különböző helyeken a beérkező jel erősségét megmérve majd út és csillapítás számításokat végezve a forrás helye körök metszéspontjainak ábrázolásával meghatározható. [171] [172] [173] [174] A csillapítási érték növekedése nyílt terepen izotróp antenna esetén arányos az adó vevő közt mért távolság négyzetével. Épületek között és azokon belül ez az érték csak komplex formulákkal modellezhető. A frekvencia és épített környezet függvényében több csillapítási formula is felírható.

Az irodalomban megtalálható az Okumara - Hata modell amely kifejezést az 4. számú egyenlet tartalmazza [175].

(4)

$$PL = 69{,}55 + 26{,}16 * \lg(f) - 13{,}82 * (h_t - h_r) - c(h_r) + \\ +(44{,}9 - 6{,}55 * \lg(h_t - h_r)) * \lg(d)$$

Ahol:

PL: terjedési veszteség (dB); f: frekvencia (MHz); d: adó és vevő közti távolság (m); h_t: adóantenna magassága (m) ; h_r : vevő antenna magassága (m) ; c(h_r) : korrekciós tényező, melynek értéke:

nagyvárosban: - $c(h_r) = 3{,}2 * \lg(11{,}75 * h_r))^2 - 4{,}97$;

kisvárosban: - $c(h_r) = (1{,}1 * lg(f) - 0{,}7) * h_r - (1{,}56 * lg(f) - 1{,}8)$

elővárosban: - $c(h_r) = 2 * (lg(\frac{f}{28}))^2 + 5{,}4$

nyílt területen: - $c(h_r) = 3{,}2(lg(f))^2 - 18{,}33 * lg(f) + 40{,}94$

Továbbá az ITU (International Telecommunication Union) gondozásában is megtalálható több formula, amelyből az ITU-R P.1238-7 02/2012 amely a 900 MHz feletti frekvenciákra lett optimalizálva. A kifejezést a 5. számú egyenlet írja le [176]

(5)

$$L_{total} = 20\, log_{10} f + N log_{10} d + L_f(n) - 28$$

Ahol:

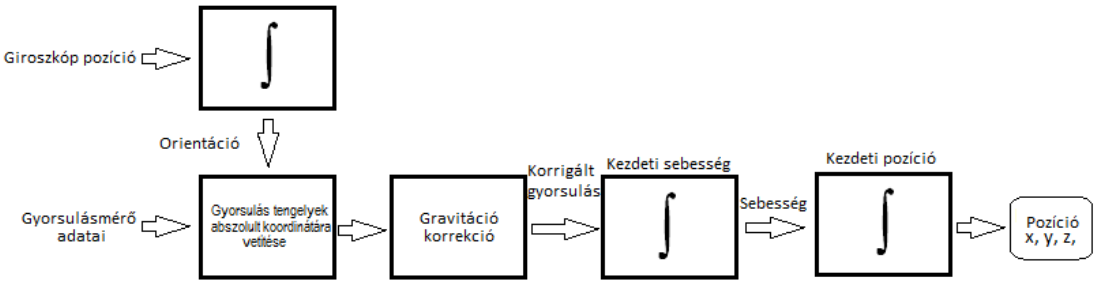
L_{total}: teljes csillapítás; N: távolság veszteségi együttható; f: frekvencia (MHz) ; d: távolság (m) az adó távolság és a mérőterminál között (ahol d>1m) ; L_f= padló csillapítása (dB) ; n: emeletek száma az adó és a mérőterminál között (n≥1)

Mint az látható, az épületeken belüli rádiós sugárforrás helyének felderítése nehéz feladat. A csillapítás mértéke, erősen a környezet függvénye.

A kutatás során egyedi elgondolás alapján, javaslatot dolgoztam ki egy kombinált mérési elv és műszer kialakítására, amely megkönnyítheti az épületeken belüli rádiós sugárforrások lokalizációját. Több ismert technológia egyidejű alkalmazásával megfelelő eredményesség érhető el vele.

5.4.13 Rádiófrekvenciás adó lokalizálása épített környezetben, saját elgondolás alapján

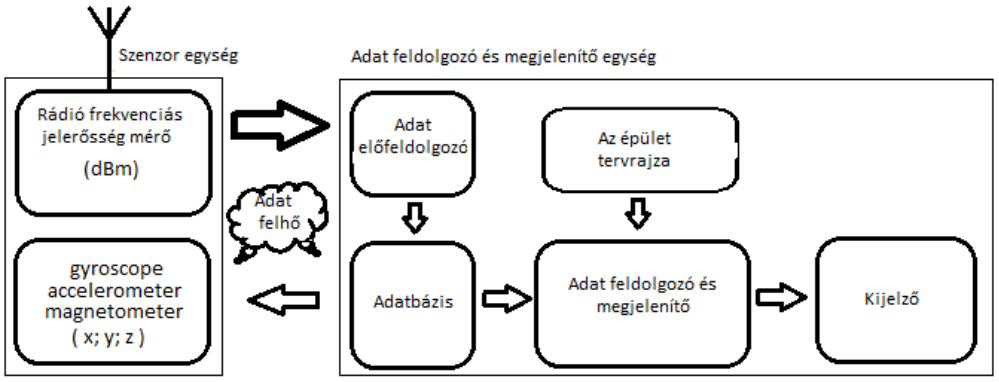
A módszer lényege abban rejlik, hogy az RSS (Received Signal Strength) módszert útvonal méréssel kombinálunk. A grafikusan megjelenített útvonal és a mért rádiós jel térerősségét együtt ábrázolva, körvonalazódik a rádiós adó térbeli elhelyezkedése. Az elképzelt berendezés egy összetett mérőegységből és egy adatfeldolgozó kiértékelő részből áll. A mérőegység a saját térbeli elhelyezkedést és a helyszínen lévő beállított rádiós jel erősségét méri. Az adatfeldolgozó kiértékelő egység a rögzített adatokat egy grafikus felületen jeleníti meg a felhasználónak. A pontos térbeli elhelyezkedés megállapítása zárt terekben, meglehetősen nehéz feladat, mivel a GPS technológia használata korlátos megoldást nyújthat. [177] Ezzel szemben a mérésének egy lehetséges megoldása az inerciális navigáció lehet. Az inerciális navigációs rendszerek működésének elve a fizika azon jelenségeinek alkalmazásán alapszik, amelyek a testek gyorsuló mozgásakor lépnek fel, ha a test mozgását valamely álló derékszögű koordináta-rendszerben vizsgáljuk. Az inerciális navigációs rendszerek mérésére gyorsulásmérőket „accelerometereket" alkalmazunk. Napjainkban elérhetővé váltak olyan kisméretű IMU (Inertial Measurement Unit) szenzorok, amelyek alkalmazása és pontossága elégséges lehet a feladat megvalósításához. A szenzorok működésüket tekintve komplex funkciókat valósítanak meg, gyorsulás, elfordulás és elektromágneses térerő adatokat szolgáltatva. A mérési elgondolás szerint a helymeghatározáshoz feltétlenül szükséges koordinátákat a gyorsulásmérők jeleinek idő szerinti második integráljából számolhatjuk ki. A folyamatot a 68.számú ábra szemlélteti. [178] [179] [180]



68. ábra Giroszkóp alapú pozíció meghatározás Forrás: [180] 4. ábrája alapján

A mérési elgondolás alapján a giroszkóp egységet összeépítve egy körvételi antennával felszerelt szoftverrádióval, a helymeghatározással párhuzamosan egy időben a keresett

frekvenciájú és sávszélességű jel térerősségének mérése történik. Az előzőleg pontról pontra kiszámolt helyadatok mellé az adott térrészben lévő rádiós jel mért térerősségének értékeit rendeljük. Ezt követően a keletkező adatok egy adatbázisba kerülnek. Az adatfeldolgozás után a megvizsgált terület adott frekvencia szerinti rádiós térerősség eloszlását, három dimenzióban grafikusan ábrázolva tekinthetjük meg. A vizualizációt különböző hamis színes, -termikus megjelenítés alkalmazásával, valamint a vizsgált terület tervrajzainak, térképeinek egymáshoz illesztésével vethetjük össze. A mérés megvalósítása és kiértékelése, előre felkonfigurált rendszer esetén nem kíván különleges szakértelmet a feladatot végrehajtó személyektől. A mérési rendszer elrendezésének elve a 69. számú ábrán látható.



69. ábra Hely alapú rádiós lefedettség mérő elrendezés Forrás:Saját ábra

A megvalósítható rendszer elképzelésem szerin két különálló egységből áll. Az elrendezést elemezve látható, hogy a kiértékelő megjelenítő egységnek nem kell a mérés helyszínén lennie és a mérési adatok kiértékelése történhet online és offline módokon is. A mérőrendszer továbbfejlesztése kapcsán, elképzelésem szerint a szenzor funkciót ellátó rádiós mérőegység kis mérete lehetővé teszi, hogy különböző autonóm robot (UAV, UGV) rendszerekbe is könnyen implementálható legyen. A módszert a műholdas helymeghatározó technológiákkal kombinálva egy olyan lokalizáló berendezéshez jutunk, amellyel gyorsan nagy területek térképezhetőek fel, megadott frekvenciájú rádiós sugárforrás felderítése érdekében.

5.4.14 Védett helyiség kapcsolódó infrastruktúrái, berendezési tárgyai

A védett helyiségek tartós kialakítása során, egy speciális célra szánt környezet megalkotása a cél. Az ember-ember közötti közvetlen kommunikáció során, a kommunikáció helyszínének illeszkednie kell a funkcionalitással és az emberek számára

meghatározó komfort követelményeivel. A védett helyiségnek és a kapcsolódó épületrészeknek ergonomikusnak kell lenniük a használhatóság szempontjának megvalósításával, illeszkedve a műszaki követelmények tarthatóságával. A védett helyiség megközelítése során a belépést biztosító biztonsági protokoll műszaki elemeinek, megfelelően nagy teret kell biztosítani a kényelmes bejutás elősegítése érdekében. Rendelkezni kell megfelelő pakoló és biztonsági tároló kialakításokkal. A védett helyiségbe történő belépést követően a megfelelő terek kialakításával, a belső látszó falazatnak illeszkednie kell a kor elvárásainak, tárgyaló jelleget teremtve a létesítmény kialakításának. A bútorzat megválasztásánál is kettős követelmény kielégítése a cél, az ergonomikus használat, valamint az átvizsgálhatóság, könnyű áttekinthetőség szempontjai. A védett helyiség bútorzatát tekintve nem szabad, hogy túlzsúfolt legyen. Az anyaghasználat tekintetében az átlátszó műanyag (PLEXI) és üveg anyagú berendezési tárgyak megfelelő megoldást nyújthatnak. Törekedni kell a bútorok teherhordó részeinek üregmentes kialakítására. A védett helyiségek tekintetében, a pontos helyiségleltár megoldást nyújthat a dedikált bútorzat kialakításához, hogy a bútorok az idő múlásával is a védett helyiség azonosított részei maradjanak.

A védett helyiségek kialakítása során, a megfelelő világítás tervezése szintén fontos feladat, mivel a huzamos emberi tartózkodás feltétele. A világítás kialakítása kapcsán fontos az áttekinthető, egyszerű felépítésű lámpatest felhasználása. Kerülendő az elektronikus gyújtóval ellátott, elektromos zajt termelő előtétek használata. A hagyományos izzószálas fényforrás jelenthet megfelelő megoldást. A belső elektromos hálózat és az energiaátviteli szűrő méretezése során a fényforrások energiaigénye számottevő lehet, ezért fontos a méretezés és az előre tervezett kialakítás.

5.4.15 Védett helyiség légcseréjének kialakítása

A kialakított védett helyiségben történő tartós emberi tartózkodás feltétele, a megfelelő légcsere kialakítása. A védett helyiségek kialakításának rádiófrekvenciás árnyékolása kapcsán felmerül az árnyékolás homogenitásának megszakításával járó csillapítási nehézségek problémája, azonban a helyiség emberi tartózkodásra történő kialakítása kapcsán a helyiség légcseréje nélkülözhetetlen megoldandó feladat. A megoldást a külső környezetből történő, árnyékoló honeycomb szellőzőkön keresztül történő kialakítás jelenti. A külső környezetből történő légutánpótlás megvalósítása során, a gépészeti légvezeték kialakítása folyamán ügyelve az információbiztonsági kockázatok

kiküszöbölésére, kialakítható a tartós légcsere követelménye. A védett helyiség belső hőmérsékletének szabályozására szintén a befújt levegő hőmérsékletének változtathatósága adhat megoldást, illetve kompromisszumként a védett helyiség belső környezetében elhelyezett villamos fűtés lehet a további megoldás.

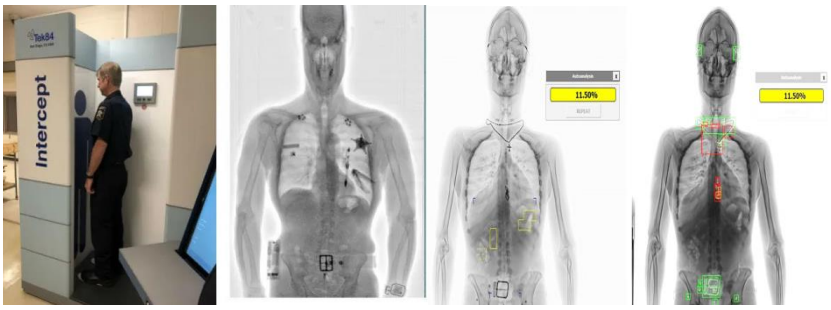
5.4.16 Védett helyiségbe történő beléptetés és személyátvizsgálás

A védett helyiségek használata során alapvető elvárás a helyiség folyamatos rendelkezésre állása az ember-ember közötti kommunikációs interaktusok lebonyolítása érdekében. Ezért első lépésként a résztvevő felek használati jogosultságának megállapítását kell végrehajtani. A használat során a védett kommunikációra érkező személyek közül feltételezhetőleg az egyik fél a létesítmény üzemeltetését végző intézmény dolgozója (dolgozói), míg a másik fél (felek) a legkülönbözőbb helyekről érkezhet (érkezhetnek). Első körben célszerű lehet megbizonyosodni az érkező tárgyaló fél (felek) személyazonosságáról. A személyazonosság egyszerű megállapításának teljesen természetesnek kell lennie, mivel a legegyszerűbb ügyintézés során is minden esetben elkérik okmányainkat. A beléptetés tényét, a védett helyiséghez köthető megfigyelő rendszeren kívül írásos naplóban is célszerű vezetni, amely szerves kísérő dokumentumát jelenti a védett helyiségek üzemvitelének. Az azonosítási és regisztrálási folyamatot követően, a védett helyiségben folytatott kommunikáció bizalmasságának érdekében ki kell zárni annak lehetőségét, hogy a helyiségbe bármilyen véletlen vagy szándékos módon, személyes vagy ajándéktárgy útján, idegen, ismeretlen funkciókat rejtő technológia kerülhessen. Ennek legmegfelelőbb megoldása a védett helyiségek szoros környezetében, az adminisztratív zónában létrehozott technikai beléptetési pont kialakítása. A beléptetésnek az általános objektumbeléptetéssel szemben specializáltnak kell lennie. A beléptetés során természetesen nem a megszokott eszközöket kell keresni, hanem a védett kommunikáció esetleges offenzív technikai támadására alkalmas tárgyakat. A védett kommunikációra érkező feleknek személyátvizsgáláson javasolt átesniük. A ruházat, átvizsgálás mellett figyelemmel kell lenni az órák, ékszerek, tárcák tartalmára, mivel a témában felemrülő támadóeszközök kinézete a legváltozatosabb miniatürizált formákat vehetik fel, illetve a személyes kommunikációs eszközök biztonságos működése nem garantálható. A védett helyiségek környezetében célszerű megfelelő méretű lemezszekrényt és fém tároló-kazettákat rendszeresíteni a nem eldönthető, a védett helyiségben folytatott kommunikáció lefolytatásához nélkülözhető

tárgyak elzárása érdekében. Fontos, hogy a védett helyiségbe érkező személyek együttműködőek legyenek a védett helyiség üzemeltetésével megbízott személyzettel, mivel a kommunikáció bizalmasságának alapvető feltétele a bizonytalan kockázati tényezők kizárása.

A személyátvizsgálás elterjedt, hagyományos technikai eszközrendszere többnyire fémérzékelő detektorokból álló kézi és telepített eszközrendszer, azonban napjainkra, ugyan költségesebb megoldás révén, kifinomultabb megoldások is kínálkoznak az emberi test felületéhez közel lévő idegen anyagok kimutatására. Ezek az eszközök már nem csak kimondottan a ferromágneses fémes tárgyak kimutatására alkalmasak. A piacon megjelenő új személyátvizsgáló eszközöket szemügyre véve, a technikai eszközök felderítésére hangolva, több megfelelő korszerű lehetőség is kínálkozik. Az egyik az NLJD (Non Linear Junction Detectors) félvezető átmenet detektáló kapu és kézi szkenner, melyek kimondottan félvezető alapú eszközöket (pl.: tranzisztor, integrált áramkört, mobiltelefon, SIM kártya, stb.) tartalmazó eszközök kimutatására lettek kifejlesztve. A másik a testszkenner berendezés, amely minden a testfelszínhez közeli tárgy kimutatására alkalmas a ruházat eltávolítása nélkül. Az NLJD kapu kialakításai a 70. ábrán látható, míg a testszkenner és vizsgálati képei a 71. ábrán látható.

70. ábra NLJD kapu Forrás: [181]



71. ábra Testszkenner megjelenítési képpel, valamint kimutatható találatok Forrás: [182] [183]

Működési módjuk tekintetében a hagyományos beléptető kapuk és szkennerek a közelükben érzékelt mágneses anyagok okozta, a kapu és kézi szkenner áramköreiben változást létrehozó jelenségek különbségeire adnak riasztási jelzést. Míg a félvezető átmenet és test szkenner berendezések nagyfrekvenciás jelek kibocsájtásával és az azokra érkező válaszjelek beérkezésének paramétereiből állítják elő NLJD kapu esetén a találati jelzést, míg a testszkenner készüléktípus esetén a grafikus képet.

A védett helyiségek személybeléptetéséhez, elengedhetetlen művelet a személyes tárgyak átvizsgálása, melynek korszerű formája a védett helyiség adminisztratív zónájába telepített csomagröntgen lehet. Egy ilyen berendezés és grafikus megjelenítési képe a 72. ábrán látható.

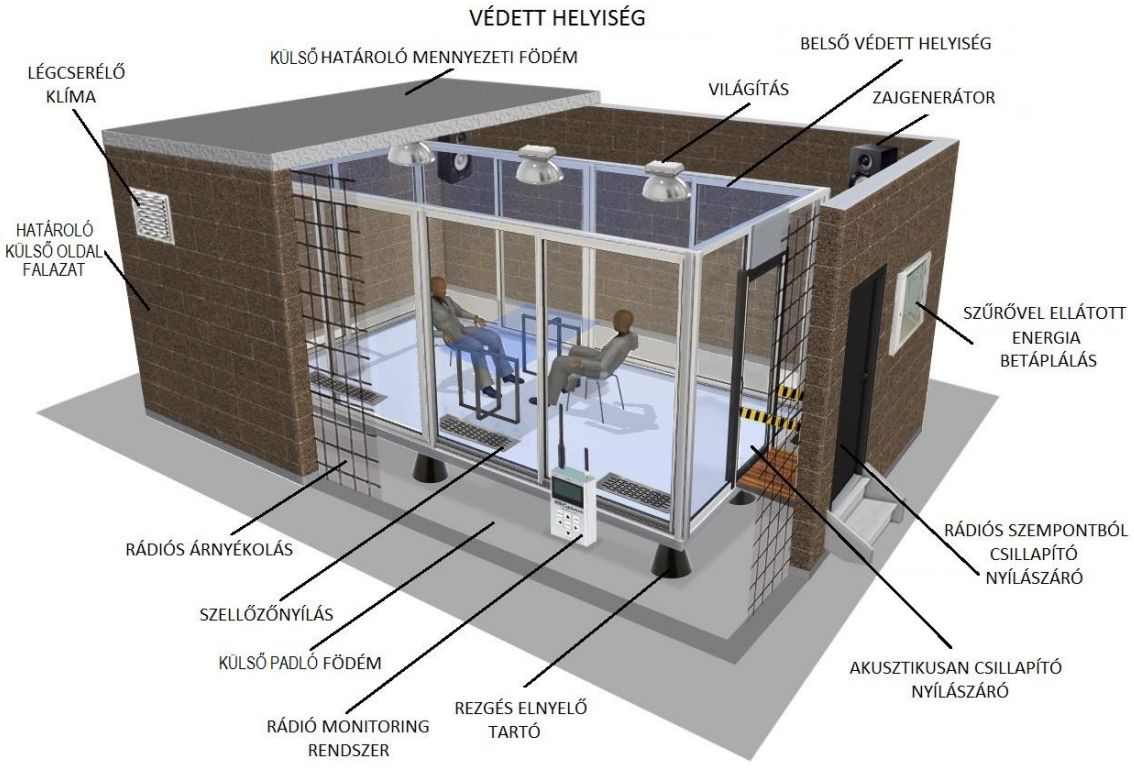
72. ábra Csomagröntgen készülék és a készített értékelési képek Forrás: [184] [185] [186]

A csomagok átvilágítása során kimutatható a személyes poggyász tartalma, amely alapján eldönthető a védett helyiségbe bevihető tárgyak és eszközök további elhelyezésének módja. A nem kívánatos vagy kockázatos eszközöket a korábban említett egyedileg zárható lemezszekrénybe, kazettába kell elhelyezni a tulajdonosnak átadható egyedi záró kulcs biztosításával. A védett helyiségek kialakítása kapcsán, kulcsfontosságú a belépő személyek kockázatmentessége, mivel a Shannon - Weaver elvi modell alapján, a védett helyiség közvetlen fizikai hozzáférésű, minőségi kommunikációs csatornájába kerülnek, ahol az információ elsődleges forrásból,

zajmentes formában áll rendelkezésre. A védett helyiségbe történő közvetlen beléptetés és személyátvizsgálás garantálhatja a minőségében megfelelő védett helyiségbe érkezők által hordozott, technikai információbiztonsági kockázat kialakulásának kizárását. Egy kialakított védett helyiségben, -tárgyalóban az újonnan bekerülő tárgyaknak műszaki tartalmi ellenőrzésen kell átesniük a nem kívánt funkciók elkerülése tekintetében. Általános irányelv, hogy ha egy tárgyat nem lehet ellenőrizni, azt lehetőség szerint nem kell a védett helyiség falai közé vinni.

5.5 A célkitűzés során meghatározott, optimális védett helyiség elvi modelljének kialakítása

A korábbi fejezetek eredményeit összegezve, valamint az eredmények összegzéséből levont következtetések alapján, bemutatom azt a védett helyiség struktúrát, melynek kialakítása, a kutatás során megismert támadásokkal szemben megfelelő ellenállóságot biztosít, a meghatározott védett helyiség definíciójának megfelelve. A védett helyiség modellje, szemléletesen a kutatás egyik eredményeként bemutatva, az elképzelésem alapján, a 3.3 fejezet 6. számú ábrája alapján történő elhelyezéssel, az alábbi 73. számú ábrán látható módon került kialakításra.



73. ábra Védett helyiség modelljének lehetséges kialakítása, saját elképzelés alapján Forrás: saját ábra

A védett helyiséget, héj modell megvalósításával, egy őrzött környezetben, új autonóm térrészként kialakítva képzelhetjük el. A védett, ember-ember közötti kommunikáció helyszínéül szolgáló térrész egy új befoglaló helyiség falain belül helyezkedik el. A tartósan kialakított védett helyiség védelmi eszközei elosztva kerülnek alkalmazásra. A helyiség kialakítását áttekintve, kívülről befelé haladva a következőeket láthatjuk:

- **Határoló külső oldal falazat.** A védett helyiség oldalirányú, szomszédos helyiségektől elválasztó határoló épületszerkezete.
- **Külső határoló mennyezeti födém.** A védett helyiség fej feletti, szomszédos helyiségektől elválasztó határoló épület szerkezete.
- **Külső padló födém.** A védett helyiség alsó, szomszédos helyiségektől elválasztó határoló épületszerkezete.
- **Rádiós árnyékolás.** A védett helyiség elektromágneses jelekkel szembeni árnyékolása. Az árnyékolás a „légcserélő klíma" honeycomb eszközön keresztül történő bevezetésével, valamint kialakított szűrővel ellátott energiabetáplálási pont kialakításával és rádiós szempontból csillapító nyílászáró beépítésével kialakítható.
- **Légcserélő klíma.** A védett helyiségben, a tartós emberi tartózkodás során szükséges légcserélés eszköze, valamint szabályozható befújási léghőmérséklet esetén a védett helyiség klimatizálásának eszköze. A légcsere „honeycomb" bevezetők használatával kialakítható.
- **Szűrővel ellátott energia betáplálás.** A védett helyiségen belül megjelenő energiaigény átvezető eszköze, amely alkalmazásával, a védett helyiség rádiós árnyékolásával illeszkedve, a védett helyiség elektromágneses árnyékolása kialakítható. A betáplálási pont paneles kialakítása esetén, eseti használatú optikai kábel átvezetése kialakítható. Az energiaellátás kábeleinek szűrővel történő ellátása, hatékony eszköz az erősáramú hálózatot átviteli útként használó megfigyelő eszközök működése ellen is.
- **Rádiós szempontból csillapító nyílászáró.** A védett helyiségbe való bejutást szolgáló nyílászáró egyik szerkezete. Az elektromágneses árnyékolás kialakításának része.
- **Két helyiség közötti tér.** A külső és belső védett helyiség közötti térrész.
- **Világítás.** A védett helyiség belső környezetének megvilágítására szolgál.
- **Rádió monitoring rendszer.** A védett helyiség belső rádiós terének vizsgálatára

és ellenőrzésére szolgáló berendezés.

- **Zajgenerátor.** A belső védett helyiségben keletkező, a külső irányba terjedő hangrezgések információtartalmának elnyomó eszköze.
- **Rezgés elnyelő tartó.** A belső védett helyiség, a közvetlen védett kommunikáció céljára létrehozott térrész statikai tartó eleme.
- **Szellőzőnyílás.** A légcserélő klíma által biztosított friss levegő, két helyiség közötti téren keresztül történő, belső védett helyiségbe jutását biztosító nyílás.
- **Belső védett helyiség.** Az információbiztonságilag védett, ember-ember közötti kommunikáció lefolytatására létrehozott térrész.
- **Akusztikusan csillapító nyílászáró.** A belső védett helyiségbe való közvetlen bejutást szolgáló nyílászáró másik szerkezete, az akusztikus csillapítás kialakításának része.

Az ábrán szemléltetett helyiségek kialakítása és elemeinek funkciója a következő: Az új térrész külső falazatát, mennyezetét és padló födém szerkezetét, az előző fejezetekben ismertetett módon szilárd építőanyagok felhasználásával kell kialakítani. A határoló részek kialakítása során több szempont figyelembevétele javasolt. Figyelembe kell venni a befoglaló méretek nagyságát, statikai szempontból a belső védett helyiség kialakítása során jelentkező plusz tömeget, valamit az akusztikus csillapítás kialakításának igényét, amellyel a védett helyiségben előálló akusztikus rezgések útja csillapítható.

A külső falazat kialakítása során célszerű olyan megoldást keresni, melynek alkalmazása során a megbontás- helyreállítás nyomai detektálható. Az nyomok nélkül ne legyenek megvalósítható. Erre különböző keménységű, homogén strukturált anyagok megfelelőek lehetnek, valamint festékbevonatok alkalmazhatóak. A külső és a belső tereknek minden irányból átjárhatónak kell lenniük a későbbi ellenőrzések és karbantartások megvalósítása érdekében.

A rádiós hullámok okozta kockázatok kizárása céljából, az árnyékolás kialakítását a külső helyiség belső felületén célszerű kialakítani. A kialakítás így oly módon megvalósítható, hogy az védett lehet a külső környezetből érkező mechanikus behatások ellen, valamint belülről hozzáférhető marad a későbbi ellenőrzések során. A rádiós szempontból történő árnyékolás a kutatás előző részeiben taglaltak alapján, hatékony védelmet nyújt a védett helyiségen belül, az esetlegesen keletkezett rádiós jelek továbbterjedése és a kintről érkező kommunikációs csatornák védett helyiségen belüli

elérésének megakadályozása céljából. Továbbá elősegíti a védett helyiségen belül működő rádiós ellenőrzőrendszer hatékony működését.

A belső védett helyiség légcserélését a külső helyiség falazatán keresztül, a külső tér irányából célszerű megoldani. Az elképzelés alapján az érkező friss levegő közvetett módon érkezik a belső tárgyaló légterébe. A légcsere a közvetlen külső térrel való kapcsolat elkerülése érdekében a belső védett helyiség eltolt szellőzőnyílásain keresztül valósulhat meg. A légáramlás a külső határoló épületszerkezet nyílásain, a rádiós árnyékolás megtartása mellett, méhsejt szerkezetű légátvezetők alkalmazásával kialakítható.

A belső védett helyiség és külső határoló szerkezet közötti térrészbe, valamint a gépészet légcsatornáiba zaj generálása célszerű, a belső helyiségben keletkező hangrezgések tiszta tovaterjedésének megakadályozása céljából. A külső körülvevő helyiség falazatát felül kell vizsgálni a bent keletkező hang csillapításának mértéke szempontjából. Az akusztikus módon terjedő rezgések információtartalmának gyengítése céljából a határoló falazat zajt sugárzó transzducer rezgéskeltők alkalmazásával is ellátható.

A belső védett helyiség világítása, a külső védett helyiség mennyezeti födémjén elhelyezett világítótestek alkalmazásával megoldható, fényvezető anyagú belső védett helyiség mennyezet kialakításával. Ezzel a megoldással biztosítva a belső védett helyiségben használt műszaki berendezések számának csökkentése. A világítótestek fényforrásainak célszerűen izzószálas kialakításúnak kell lenniük a termelt elektromágneses zaj elkerülése céljából.

A belső védett helyiségbe történő bejutást kettős nyílászáró szerkezet biztosíthatja. A külső határoló falazaton a helyiség rádiós árnyékolásával egy rendszerben lévő rádiófrekvenciás csillapító nyílászárón keresztül juthatunk, amellyel az akusztikus csillapítása is fokozható. Ezt követően a belső védett helyiség falazatába épített, elsődlegesen akusztikusan csillapító nyílászárón keresztül juthatunk. A belső védett helyiség, egy különálló homogén határoló épületszerkezetekkel ellátott helyiséget képvisel. Ez a térrész szolgál a védett kommunikációs interraktus lebonyolítására.

A belső védett helyiség falazatának homogénnek és teljesen elektromos technológiamentesnek kell lennie. Erre megfelelő megoldás lehet az üvegből-plexiből történő kialakítás.

A belső védett helyiségnek, az akusztikai süket terekhez hasonlóan csillapító rezgés elnyelő tartókon kell állniuk. A kialakítás során törekedni kell az üregmentes tartószerkezeti elemek használatára, valamint a ragasztás technológiájára. A belső védett

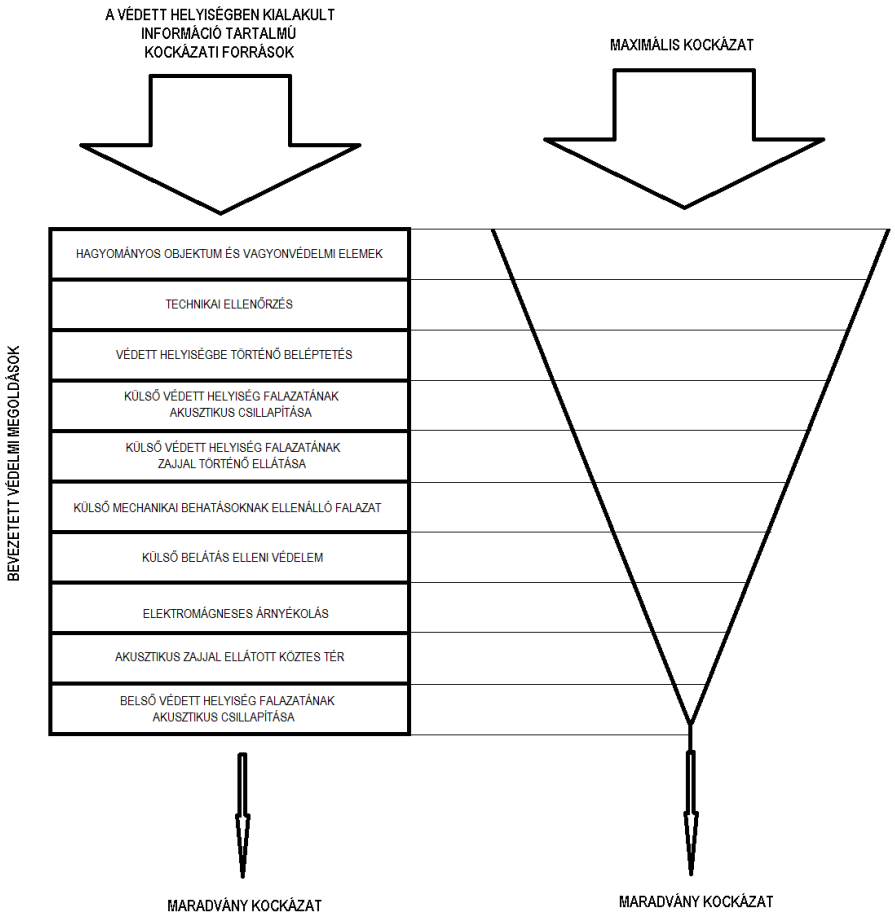
tér üvegszerkezet alkalmazása esetén, egyik felületén mart felületű (fehér) lehet, amely alkalmazása révén, a fényáteresztő tulajdonsága megmarad. Az ilyen kialakítás révén, külön takaróelemek felhasználása nélkül teljesíti a kellemes küllem kialakításának igényét, takarva a külső védett helyiség belső felületén elhelyezett rádiós árnyékolás struktúráját. Az üveg alapú belső védett helyiség kialakítás további lényeges tulajdonsága, hogy a technikai átvizsgálás- karbantartás esetén könnyen áttekinthető, annak homogén és átlátszó tulajdonsága miatt. Ezzel biztosítva a könnyű ellenőrizhetőség feltételét. További előnye a jól tervezhető akusztikus csillapítás.

A védett helyiség berendezési tárgyait tekintve az egyszerűségre kell törekedni. A berendezési tárgyak minél kisebb mértékben tartalmazzanak fémet, lehetőség szerint üveg és átlátszó plexiből készült bútorok alkalmazásával, ezáltal törekedve a könnyű átvizsgálás megvalósíthatóságára.

A védett helyiséget úgy célszerű kialakítani, hogy a helyiségbe való bejutás egy, a külső védett helyiség tulajdonságaival megegyező adminisztratív zónán keresztül történjen. (A 73. ábra nem tartalmazza).

A védelem kialakítása során törekedni kell a helyiségkomplexum megfelelő zárral és beléptető rendszerrel való ellátására. Az elektronikus vagyonvédelem kiépítése során autonóm kamerás megfigyelő rendszer és elektronikus vagyonvédelem kialakítása javasolt a központi rendszertől elkülönített formában. Az autonóm, kizárólag a védett helyiség üzemeltetéséhez kapcsolódó berendezéseket a kialakított adminisztratív zónában helyezhetjük el. A mechanikai védelmet és elektromágneses árnyékolást megvalósító falazat, valamint a kommunikáció helyszínéül kialakított belső védett helyiség közötti térrésznek minden irányból átjárhatónak kell lennie az átvizsgálás-karbantartás hatékony megvalósíthatóságának céljából.

A védett helyiség rádiós felügyeletét a köztes térben elhelyezett mérőkészséggel végezhetjük, az adminisztratív zónában kialakított vezérlő kialakításával. A bevezetett védelmi megoldások struktúrája, az előzőektől eltérő módon ábrázolva, az alábbi 74. ábrának megfelelően csökkentik a maradványkockázat értékét.



74. ábra Védett helyiség struktúrájának hatása a maradványkockázat mértékére Forrás: saját ábra

A védett helyiségek megvalósítása során, a következő alapvető paraméterek meghatározása szükséges a tervezői munka megkezdéséhez:

- A védett helyiség kialakításának szükségessége;
- A kialakítani kívánt védett helyiség épületen belüli elhelyezésének tervezett helyszíne, helyszín kiválasztása;
- A használható anyagok típusai a kialakítás során;
- A kialakítani kívánt védett helyiség belső mérete, területe, belső magassága;
- A belépési pontok száma;
- A védett helyiséget egyidejűleg használó személyek száma;
- Szükséges légtechnikai igény;
- A kialakítás alapvető szempontjai, lehetséges módjai, kiemelt figyelemmel a nyílászáró, hálózati szűrő és légtechnika kialakítására;
- Elhelyezni kívánt elektronikus eszközök hűtési igénye;
- Elhelyezni kívánt elektronikus eszközök teljesítményigénye;
- Belső megvilágítás mértéke;

- A biztonság állapotát fenyegető tényezők megakadályozására és észlelésére használt berendezések és funkciók;
- Elektromágneses csillapítás mértéke;
- Földelés és villámvédelem kialakításának szükségessége;
- A védett helyiség falazatának készítése és rongálódás detektálhatóságának kialakítása;
- Védett helyiség falazatával kapcsolatos mechanikai ellenállóság mértéke a mennyezetet és a padlót is beleértve;
- Védett helyiség falazatával kapcsolatos akusztikai csillapítás mértéke a mennyezetet és a padlót is beleértve;
- A berendezési tárgyak, valamint bútorzat igénye;
- Önálló elektronikus vagyonvédelem kialakításának igénye;
- Mechanikai védelmi igények;
- A kialakított védett helyiség kialakítást követő bemérése és üzembe helyezése;
- A kialakított védett helyiségbe történő üzemszerű beléptetés lehetőségének megteremtése;
- A védett helyiség folyamatos üzeméhez tartozó követelmények és intézkedések meghatározása
- Tűzvédelem.

A védett helyiség megvalósításához szükséges tervek:

- A védett helyiség épületen belüli elhelyezése, a megvalósítás helyszíne;
- Alapmérettől függő határoló szerkezeti változtatások terve, tekintettel a födémterhelési értékekre;
- Statikai megerősítés terve, annak szükségessége esetén;
- A védett helyiség határoló épületszerkezeti elemeinek kialakítása az akusztikai csillapítás kialakításához, szükséges anyagok típusa, vastagsága, összhangban az esetleges határoló szerkezeti változásokkal;
- A védett helyiség határoló épületszerkezeti elemeinek kialakítása az elektromágneses csillapítás kialakításához, szükséges anyagok típusa, vastagsága;
- Belső burkolatok rögzítése a padozat és a mennyezet tekintetében;
- Belső védett helyiség szerkezeti terve;

- Belső védett helyiség akusztikai rezgéseket csillapító tartószerkezetének kialakítási terve;
- Légtechnikai betáplálás, légcsere módja, összhangban a hűtés-fűtés kialakításával;
- A belső hőmérséklet temperálásához szükséges légtechnikai eszközök méretezése, kialakítása;
- Erősáramú és jelvezeték szűrők alkalmazásának terve, teljesítmény meghatározása, méretezett kábelkeresztmetszet és mennyiség;
- Önálló elektronikus vagyonvédelem terve;
- Mechanikai vagyonvédelmi elemek terve.
- A helyiség jellemzőinek mérési terve;
- Az üzemszerű beléptetés terve;
- A védett helyiség használatának és technológiájának leírása, tekintettel az ember-ember közötti biztonságos kommunikáció megvalósítására;
- Tűzriadó terv.

A védett helyiség ily módon történő kialakítása ellenálló megoldást nyújt a kutatás során feltárt, az ember-ember közötti kommunikáció során felmerülő technikai jellegű információbiztonsági kockázatok kizárására tett elvárásoknak.

ÖSSZEGZÉS

Jelen fejezetben a hipotézisek hatodik és hetedik pontjában feltételezett környezet kialakítása és technológiai megoldása került kidolgozásra, ami alapján a hipotézis került bizonyításra. A fejezetben a korábbi fejezetek eredményeit felhasználva került kifejtésre a védett helyiség kialakításához szükséges intézkedések komplex struktúrája. A komponensek áttekintése elengedhetetlen feltétele a védett helyiségek kialakításának, mivel azok jellege döntően befolyásolja a kialakítani kívánt helyiség színvonalát. A védett helyiség elhelyezése szempontjából, lehetőleg olyan épületrészben kerüljön kialakításra, amely a külső környezettől távol helyezkedjen el. A környező szomszédos épületrészek legyenek bejárhatóak minden irányból az ellenőrizhetőség megvalósítása érdekében. A kialakítás során szempont, hogy amennyiben lehetséges, a védett helyiség elzárt legyen a külvilágtól. A védett teret őrzött tér vegye körül a héj szerkezet megvalósítása érdekében. A védett helyiséget határoló felületek, lehetőség szerint tégla vagy betonból készüljenek, burkolatok nélkül. A helyiség határoló felületeinek kialakítása során, figyelemmel kell lenni a hangszigetelés kialakítására értékek meghatározásával. A kialakítás során biztosítani kell a helyiség elektromágneses csillapítását, tekintettel a frekvenciatartomány és a csillapítási értékek meghatározásával. A védett helyiség nyílászáróit, megfelelő minőségű mechanikus védelemmel kell ellátni, önálló elektronikus vagyonvédelemi rendszer kialakítása mellett. Az információbiztonság megteremtése érdekében, a védett helyiség határoló falazatát elektronikus zajgenerátorral célszerű ellátni, a falazat rezgései útján terjedő információtartalmú jelek elnyomása céljából. A légtechnikai csövezés csatornáiba akusztikus sugárzók elhelyezése szükséges, a terjedési csatorna lezárása céljából. A védelmi eszközök vezérlése, a védett helyiséggel azonos védelmi szintnek megfelelő védett zónájából kell hogy kialakítva legyen. A zajforrásoknak fehérzaj jellegű zajt kell, hogy sugározzanak. A védett helyiségek kialakítása során, rádiófrekvenciás zavaró eszköz alkalmazása nem javasolt a törvényi korlátozásoknak megfelelve. A védett helyiségben elhelyezett tárgyak tekintetében a bútorzatot tekintve könnyen átvizsgálhatónak kell lennie. Anyaguk tekintetében főként transzparens anyagból készüljenek. A helyiségben használt berendezési tárgyakat, eszközöket, oly módon célszerű megválasztani, hogy azok megbontása, szétszerelése valamint dedikált elhelyezése egyértelműen detektálható legyen. A szükséges informatikai és technikai eszközöknek az információbiztonság szempontjából megfelelőnek kell lenniük. A védett

helyiségben lévő tárgyakról, pontos leltár felvétele szükséges rendszeres ellenőrzés mellett. A védett helyiségben lévő tárgyakat, egyedi azonosítókkal szükséges ellátni. A védett helyiségekben a műszaki eszközök jelenlétét minimalizálni szükséges, a telekommunikációs eszközök használatának erőteljes korlátozása mellett. Amennyiben mégis, a védett kommunikációhoz nélkülözhetetlen műszaki berendezés használata válik szükségessé a védett térben, úgy azt csak szakszerű átvizsgálást követően, megfelelőség esetén lehet a helyiség falai közé vinni, lezárva, a leltárban feltüntetve, a helyiség üzemeltetési naplójában rögzítve.

Megállapítom, hogy a védett helyiségek kialakítása során a helyiségben alkalmazható egyetlen megfelelő adatátviteli- adatkapcsolati technológia fizikai rétege az optikai szál lehet. A technológia adta lehetőségek miatt, az információbiztonsági szempontból védett helyiségek fizikai rétegeként, az optikai szál fizikai állapota folyamatosan monitorozható, mellyel a külső behatások okozta állapotváltozások azonnal kimutathatóak. A kapcsolódó fejezetrész, a témában végzett kutatást összefoglalja, illetve a fejezethez kapcsolódó, 2. számú melléklet az optikai szálak méréséhez és monitoring rendszereihez kapcsolódó alapelveket taglalja.

A védett helyiségek belső gépészeti elemeinek tekintetében és a vezetékezés kialakításai során, olyan megoldásokat kell alkalmazni, amelyek falon kívüli, látszó szereléssel megvalósíthatóak, lehetőség szerint transzparens anyagok felhasználásával. Az elektromos rendszert, az elektromágneses árnyékoláshoz illeszkedő szűrővel ellátva, a külső hozzáférés lehetőségét megakadályozó kivitellel kialakítva. A légtechnikát az elektromágneses árnyékoláshoz illeszkedő, légátvezetők beépítésével szükséges létesíteni, elektronikamentes kialakítással. A helyiség fűtését-hűtését lehetőség szerint a légbefúvó berendezéssel célszerű megoldani, szükség esetén a védett helyiségben elhelyezett elektromos fűtés kialakításával. A védett helyiségben az el, és átmenő gépészeti csövek kialakítását mellőzni szükséges, a csövek miatt kialakuló információszivárgási csatornák kizárása céljából. A védett helyiséget egyedi biztonsági rendszerrel célszerű ellátni, amely autonóm rendszerként működik, külön a központi felügyeleti rendszertől. A helyiséget, az üzemeltetésért felelős, korlátolt létszámú személy-személyek kijelölésével szükséges működtetni, a számukra megfelelő, a védett helyiség üzeméhez szükséges tudás ismeretével. A helyiség üzemeltetése során az üzemeltetési rend kialakítása szükséges, amely intézkedések a jelentkező használati igények, takarítási tevékenység, karbantartás, rendkívüli esemény menetrendjét határozza meg. A védett helyiség időszakonként, valamint a helyiség használatával

összefüggő biztonsági incidens esetén, technikai ellenőrzésen, vizsgálaton, karbantartáson kell, hogy átessen, a helység állapotának, valamint paramétereinek újbóli vizsgálatával, a megfelelőség igazolása helyreállítása céljából.

A védett helyiségnek a létrehozás céljának megfelelően, a munkavégzés rendjéhez illeszkedve, a védeni kívánt kommunikáció céljára elérhetőnek kell lennie. A karbantartás és ellenőrzés elvégzését, a használó csoport munkarendjétől eltérő időben kell végezni a nyilvánosság kizárásával. A védett helyiség, a fejezetben részletezett módon történő kialakításával, a helyiség garantálja a falain belül lebonyolított közvetlen ember-ember közötti biztonságos kommunikáció megvalósításának lehetőségét, valamint az elhangzó és vizuálisan megjelenő információ bizalmasságát.

A jövő védett helyiségeinek paramétereit elképzelve, a következő elképzelések mentén kerülhetnek kialakításra: A jövő védett helyiségeinek környezetét véleményem szerint az elképzelésemhez hasonlóan, szenzorokkal felszerelve kell kialakítani. A szenzoroknak intelligens módon figyelniük kell a körülöttük lévő tér paramétereit. A szenzorok lehetnek rádiós mérőberendezések, amelyek az étert monitorozzák, a rádiós kisugárzások aktivitását érzékelik, valamint értékelik, de lehetnek szeizmikus és hang azonosítók is, megfelelő biztonsági garanciák megteremtése mellett.

Az anyagtechnológia fejlődésével új típusú alapanyagok is napvilágra kerülhetnek, például olyan anyagok, amelyek sérülése esetén önregeneráló módon viselkednek. A vágást vagy törést maguktól helyreállítják, nem tartják magukban az idegen tárgyakat.

Megoldás lehet olyan technológia kialakítása is, amely az adatszivárgás lehetőségét detektálja és felfedi. Ez lehet olyan berendezés megalkotása, amely egy bizonyos kiterjedésű térrészben megakadályozza a ma ismert adatszerző technológiák működését.

A mesterséges intelligencia rohamos fejlődésével, az MI technológiát az információs társadalom adatfeldolgozó egységei szinte biztosan használni fogják. Elképzelhető, hogy a védett helyiségekben alkalmazott döntéstámogató eszközök, mesterséges intelligenciával fognak rendelkezni a jövőben.

A megjelenő új kockázatok tükrében lehetséges, hogy a mesterséges intelligenciával felvértezett eszközök biztonsági résként fognak jelentkezni.

Századunk anyagtechnológiai csúcsa a nanotechnológia által különleges, eddig még nem ismert berendezések megalkotása válik lehetővé, amelyek a védelmi intézkedések eddig még nem ismert formáit hozhatják a védett helyiségek biztonságának növelése érdekében.

VI. ÖSSZEGZETT KÖVETKEZTETÉSEK

Kutatásom fókusza az ember-ember közötti személyes, bizalmas kommunikáció lefolytatásának helyszínéül kialakítható, zárt környezet megteremtésének kialakíthatóságát célozza. Az értekezés a kutatás folyamatát és eredményeit V. fejezeten keresztül, a kitűzött célok mentén, strukturáltan mutatja be.

Az értekezés I. fejezetében áttekintem az adat és információ kapcsolódásának elméleti hátterét, az információ értékké alakulását, a kapcsolódó információs architektúra piramis modellje révén. Megvizsgálom és tisztázom az egy térrészben lévő, közvetlen ember-ember közötti kommunikáció során fellépő, valamint a kommunikációt segítő technikai megjelenítő elemek által létrehozott fizikai jelenségeket, mely jelenségek a kommunikáció információtartalmát magukkal hordozzák, információbiztonsági aggályokat létrehozva. Megjelenítem a kommunikációs interakcióból származó fizikai jelenségek védelmének igényét, amely alapot teremt a védett helyiség kialakításához. A fejezetben meghatározásra kerül a felmerülő biztonsági rés meghatározása, valamint a téma szempontjából mérvadó védett helyiség fogalma, alapot teremtve a kutatás további részeinek.

A II. fejezetben áttekintem az elérhető jogalkotói intézkedéseket, melynek során igazolom a feltevésem. A kutatás idején, a Magyarországon hatályban lévő elérhető előírások tekintetében, nincs a téma kontextusában mérvadó, megfigyelés ellen védett helyiség műszaki kialakítására egyértelmű utasítás. A megállapítás tovább erősíti a kutatási célt, azaz a műszaki intézkedésekkel védett környezet kialakításának relevanciáját. A fejezetben áttekintem a védelem és a biztonság kapcsolatát, illetve a védelmi intézkedések kialakítására vonatkozó gazdasági megfontolást, amely alapján mérlegelhető a kialakítás szükségessége a felmerülő kockázatok függvényében.

A védelem kialakításának összetevői, és a kialakításra szánt beruházás értékének optimum metszéspontja alapján, megjelölhető az a pont, amely alapján a védett helyiség maradványkockázati értéke a legkisebb mértékű. A védett helyiségek jelentősége és kialakíthatósága tekintetében meghatározhatóak azok a szektorok, ahol mérlegelendő a védett helyiség kialakítása. Feltételezésem alapján egyaránt javasolom és szükségesnek tartom az állami és magán szektorok intézményrendszereihez kapcsolódóan, melyek létfontosságú (kritikus) infrastruktúrák intézményei, kapcsolódó részei, valamint a védett helyiség kialakításával nagyságrendben egyező értékű eszmei és gazdasági információs értékkel rendelkeznek. A védett helyiségek kialakítása, összetett feladat,

melynek kialakítása kapcsán több tudományterület együttműködése szükséges. A fejezetben a kapcsolódó tudományterületeket érintő jelleggel áttekintem.

A védett helyiség elhelyezése és a fizikai kialakítás kerül a továbbiak fókuszába. Áttekintem az objektumvédelem hagyományos elemeit, majd megvizsgálom a védett helyiség épületen belüli elhelyezésének optimális lehetőségeit, az előzőekben besorolt állami és magán szektorban megvalósítható struktúrát alkotva. Ezt követően javaslatot teszek egy védett helyiség objektumon belüli elhelyezésének lehetséges módjára, valamint az autonóm védelmi infrastruktúra kialakítására.

A következő IV. fejezetben csoportosítást végeztem a hírszerzés módszereinek tekintetében. Különválasztva a humán és technika módokat, megjelöltem az elektronikus információszerzés elemei között a célirányt, a lehallgatást, amely elsődleges kockázatot jelent a védett helyiségben keletkező információtartalomra nézve. Továbbá áttekintettem a hírközlés egyetemes modelljét, melynek komponensei meghatározóak a védelmi elemek elvi szintű kidolgozása során. Az elvi áttekintést követően, gyakorlati demonstratív mérések eredményei kerülnek bemutatásra. Igazolom a közvetlen emberi kommunikációs interaktus során létrejövő hangrezgéssel egybefüggő információszivárgási csatornák kialakulását, a határoló falazatban és annak szomszédos környezetében.

Igazolom az optikai terjedés során létrejövő fény terjedésével összefüggő információszivárgási csatorna kialakulását, az optikai rálátással bíró környezetből.

Igazolom a megjelenítő eszközök nem üzemszerű rádiófrekvenciás sugárzásait, valamint a kisugárzott rádiófrekvenciás jelek sugárzásainak információtartalmát. Ezzel megjelölve az elektromágneses árnyékolás kialakításának egyik okát. Áttekintettem az offenzív alkalmazások lehetőségeit, majd rendszereztem a nyílt forrásból megismerhető fenyegetést jelentő technikai eszközök működési paramétereit, tovább elemezve a konkrét kockázatok forrásait. A fenyegetést jelentő elektronikai eszközök fő paramétereinek megismerésével, és azok csoportosításával megjelölhető az a pont, ahol a működés meggátolható. Kialakítható egy olyan struktúra, amellyel megakadályozható a kockázatot jelentő eszközök működése. Ezzel alapot teremtve a védett helyiség technikai alap paramétereinek kialakításához. Kitekintést tettem a védett helyiségeket érintő SMART-osodási folyamatok irányába, melynek során megállapítottam, hogy komoly ellentét rajzolódik ki a SMART tárgyalók és eszközök, valamint a védett helyiségekben alkalmazható megoldások között. A források elemzése alapján egy jó védett helyiség vagy tárgyaló üzemben tartása, más szemléletet kíván, mint napjaink

trendje. A gyakran ellenőrizhetetlen technológiai eszközöket háttérbe szorítva, az információs környezetre kell a fókuszt helyezni az alkalmazott berendezések ellenőrizhetőségét szem előtt tartva.

Az V. fejezetben összegzem a védett helyiségek fizikai kialakításának elvi sarokpontjait, a feltérképezett kockázati tényezőkre bevezetett védelmi megoldások többszintű meghatározásával. Elsőként áttekintem a védett helyiségek komplex biztonságának kialakításához szükséges műszaki és elvi intézkedések bevezetésének strukturált lehetőségeit, a kockázatot jelentő eszközök működésében akadályt teremtve. Ezt követően szemléltetem a biztonságos környezet eléréséhez szükséges összetevők maradványkockázat csökkentő hatását az egyes elemek ábrázolásával. A kutatás során feltérképezett veszélyforrásokat szembeállítom az ellenük bevezetett védelmi intézkedések lehetőségeivel, amelynek eredményeként a kockázatokra adott válasz konkrét eredményét szemléltetem. A védett helyiség kialakíthatósága kapcsán, áttekintem a kialakíthatóság gyakorlati lehetőségeit, amely eredményeként áttekinthető a kialakítani kívánt védett helyiség és a kockázatok csökkentésére bevezetett intézkedések kapcsolata. A kialakítás során szempont, hogy amennyiben lehetséges, a védett helyiség elzárt legyen a külvilágtól, valamint további átjárható tér vegye körül a héj típusú szerkezeti kialakítás és az ellenőrizhetőség megvalósítása érdekében. A védett helyiség kialakítása tekintetében, az egyik legfontosabb alkotó a helyiség falazata, mivel a kapcsolódó védelmi funkciók struktúrája ebben összpontosulhat. A falazat specializált jellemzőkel történő ellátásával összefüggésben, javaslatot tettem a belátás elleni kialakításra; a határoló falazat akusztikus csillapítására; a helyiség határoló falazatának akusztikus zavaró jellel való ellátására; elektromágneses árnyékolás kialakítására, valamint javaslatot teszek a csillapítások gyakorlati értékeinek megvalósítására. A védett helyiségek kialakítása során, áttekintem a rádiófrekvenciás zavaró eszköz alkalmazásának jogi hátterét, amely alapján azok alkalmazása nem javasolt a törvényi korlátozásoknak megfelelve. A védett helyiségek gyakorlati használhatóságát tekintve, a kialakítás kapcsán felmerült az alkalmankénti nyomvonalas adatkommunikáció megteremtésének igénye, melyre részkutatást végeztem. A folyamatos monitorozhatóság feltételének eleget téve, javaslatot teszek az optikai adatkapcsolat kialakíthatóságának lehetőségére. A védett helyiségek kialakítása során, a kommunikációs interaktus lebonyolításához, gyakran technikai eszközök szükségesek, melyek kompromisszum megoldások révén alkalmasak lehetnek a védett helyiségben történő kommunikációhoz. A védett helyiségek kialakítása, és üzemeltetése

elképzelhetetlen átvizsgálás és minőségellenőrző vizsgálatok-karbantartás nélkül, melyek eredményei fő jellemzői a védett helyiség biztonságos állapotának. A források alapján összegzést végeztem, melynek eredményéül vizsgálati terület és vizsgáló eszköz párosítás állítható össze, valamint felállítható a feltételezett veszélyforrások és a detektálásukra használható eszközök kapcsolata. A védett helyiség időszakonként technikai ellenőrzésen, karbantartáson kell, hogy átessen a helység állapotának, valamint paramétereinek újbóli vizsgálatával, a megfelelőség igazolása céljából. Az átvizsgálás az elvi maradványkockázat egyik leghatékonyabb csökkentésének eszköze. Kapcsolódva a védett helyiségek ellenőrzési műveleteihez a védett helyiségek környezetében lévő tér, mint lehetséges vezeték nélküli adatátviteli csatorna, folyamatos ellenőrzési feladatot kíván. A védett helyiségek közelében megjelenő új rádiófrekvenciák, információbiztonsági veszély forrásai lehetnek, amelyek keletkezési forrását azonosítani szükséges. A rádiós iránymérésre, a rádióadó helyének meghatározására több lehetséges megoldást kínálkozik, azonban azok épített környezetben való alkalmazása, a fellépő csillapítási verődési és több utas terjedési jelenségek miatt nehezen megvalósítható. A problémára megoldást keresve egy újszerű saját megoldást kívánok nyújtani, amely használható az épített környezetben történő rádiós jelek forrásainak felderítésére. A védett helyiségekbe történő személybeléptetés specializált feladat, megfelelő kialakítása szavatolja a kommunikációs eseményre érkező személyek által hordozott, ellenőrizetlen technikai eszközök védett helyiségből történő kizárását. Javaslatot teszek a védett helyiségbe történő személybeléptetés megfelelő technikai kialakítására. Az értekezés új tudományos eredményeiként, a kutatási eredményeket összegezve, modellt alkotok a felmerülő kockázatoknak ellenálló védett helyiség kialakítására. A megalkotása során a felmerülő technikai eredetű kockázatok mindegyike kizárásra kerülhet, a helyiségben létrehozható szenzitív információtartalmú ember-ember közötti kommunikációs interaktus lebonyolítása érdekében. Az elhangzott szó és megjelenő vizuális tartalom bizalmassága technikai megoldások révén szavatolva biztosítható.

Az értekezés javaslati részében általános javaslatot teszek a törvényalkotó számára a „Lehallgatás mentes környezet" vizsgálati irányainak tekintetében a „Védett helyiségek karbantartása, technikai átvizsgálása" részben felsorolt gyakorlati tartalom elemeinek javasolt figyelembe vételével.

ÚJ TUDOMÁNYOS EREDMÉNYEK

Kutatásom eredményeinek hasznosíthatósága szempontjából, megállapítható, hogy egy kevésbé publikált tudomány részterületet érintek a vizsgálódásaim során. A munkám során hét hipotézist állítok, melyek igazolásával tudományos eredményként meghatározom a „Komplex Védett Tárgyló - KVT” - védett helyiség- egyértelmű leírását, ezzel definiált terminus-technicust teremtve a témában. A fellehető források elemzése révén összegzem a technikai információszerzés módozatait és elkészítem az elektronikus információszerző eszközök csoportosítását a működési alapelvük tekintetében. A paraméterek ismeretében megállapítható azoknak az intézkedéseknek a struktúrája, melyek kialakítása során megalkotható az a környezet, amely szavatolja a technikai eszközök kockázataiból fakadó információbiztonsági rések mentességét. Konkrétan az eredményeket felhasználásával kialakítható egy védett - tárgyaló - helyiség, amely komplex intézkedések implementálása révén biztonságos környezetet nyújt szenzitív megbeszélések számára. A védelmi elemek tárgyalása során javaslatot teszek a kialakított védett helyiségek csillapítási szintjeire, valamint javaslatot teszek az üzembe helyezés - üzemeltetés - alatti rádiófrekvenciás csillapítások mérésének metódusára.

A javaslati részben megfogalmazottak alapján, áttekintést kapunk a „lehallgatás mentes környezet” kialakításához javasolt technikai átvizsgálás rendszerére, amely komponensei a szenzitív kommunikációs környezet és a védett helyiség karbantartásának alapjául szolgálhatnak.

Műszeres méréseket végeztem, amely eredményei alapján demonstrálható a vizuális megjelenítők rádiós sugárzásainak információtartalma. Részkutatást végeztem az épített környezetben történő rádiós sugárforrás lokalizáció területén, melynek eredményéül egy rádiós mérőműszer elvi kialakítására teszek javaslatot. A rádiós mérőműszer megalkotása révén egy olyan egyedülálló képességgel rendelkező készüléket kaphatunk, amelynek alkalmazásával épületeken belüli rádiós lefedettségi térképet készíthetünk, egy kiválasztott frekvenciának megfelelően.

Részkutatást végeztem az optikai távközlés területén, melynek eredményéül átfogó képet kaphatunk a szálellenőrzési metódusok lehetőségeiről. A kutatás új tudományos eredményéül modellt alkotok a védett helyiség fizikai kialakításának tekintetében, amely ellenáll a kutatás során feltárt technikai kockázatoknak.

TÉZIS I. Definíció szerűen meghatároztam a védett helyiség fogalmát, amely egyértelmű leírást ad a kutatás tárgyát képező védett helyiség meghatározására. [K1];[K4]; [K10];[K15]; [K16]

TÉZIS II. Megfogalmazott feltevést igazolva, rendszerezhetők azok az állami és magán szektorok intézményei, melyekben az információ biztonságának egyenszilárdsága szempontjából javasolt a kutatás eredményeként létrehozott védett helyiség alkalmazása. [K2];[K4];[K8];[K14];[K15];[K17]; [K19]; [K23]

TÉZIS III. Megfogalmazott felvetést igazolva, meghatároztam a védett helyiségek elhelyezésének és kialakításának általános struktúráját. [K2];[K3]; [K4]; [K8]; [K17]; [K19]; [K23]

TÉZIS IV. Feltételezésem negyedik pontját analitikus kutatási stratégiát folytatva igazoltam, hogy a nyílt felületeken elérhetőek egyedi eszközös elektronikus információszerző eszközök, amelyek működési alapparamétereik szerint rendszerezhetőek. A rendszerezés során meghatároztam a működés rendszertanára vonatkozó alapelvek struktúráját. Kísérleteket végeztem és megjelöltem azokat a technikai pontokat és védelmi megoldásokat, amely pontok megzavarásával, valamint technikai kialakítások bevezetésével gátolható a fenyegetettség kialakulása, közvetlen védelmi hatást kifejtve az információ megjelenésének környezetére. [K1]; [K3];[K8];[K9];[K10];[K11];[K23]

TÉZIS V. Demonstratív kísérletekkel igazoltam az ember-ember közötti kommunikáció során keletkező, a kommunikáció információtartalmával korreláló fizikai jelenségek biztonsági kockázatait. [K1];[K3];[K8];[K23]

TÉZIS VI. A védett helyiséget a kutatás során megalapozott védelmi kialakításokat implementálva, modell készítésével bizonyítottam, hogy komplex megoldások révén, létrehozható egy olyan környezet, amely a kutatás során megismert, biztonsági kockázatokat hordozó jellemzőknek ellenáll, valamint létrehozható egy olyan tevékenységi protokoll, amely alkalmazásával, a biztonság fenntartását igazolva üzemeltethető egy védett helyiség. A tevékenységi protokollok kialakítása kapcsán a rádiófrekvenciás jelek lokalizálására újszerű megoldási javaslatot hoztam létre. [K3]; [K4];[K5];[K6];[K8];[K12];[K13];[K15];[K17];[K18];[K20];[K21];[K22];[K23];

[K24]; [K25]

TÉZIS VII. Dokumentumelemzéssel igazoltam, hogy meghatározható vonalas adatátviteli módszer és technológia, amely fizikai rétegét tekintve folyamatos ellenőrzés alá vonható. Kísérlettel bizonyítottam a paraméterváltozás azonnali kimutathatóságát. [K2]; [K7]; [K17]

A TÉZISPONTOKHOZ KAPCSOLÓDÓ TUDOMÁNYOS KÖZLEMÉNYEK

Tudományos folyóirat közlemények:

[K1] Bréda, Gábor; Védett helyiségek biztonságának szempontjai

KÖZTES EURÓPA: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI 8 : 1-2 pp. 157-167. , 11 p. (2016)

[K2] Bréda, Gábor ; Hajdu, Beáta; A társadalom és a védett helyiségek kapcsolata, valamint a védett helyiségek kialakításához kapcsolódó tudományterületek

KÖZTES EURÓPA: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI 9 : 1-2 pp. 89-96. , 8 p. (2017)

[K3] Bréda, Gábor; Védett tárgyaló kialakításának alapvető biztonsági kérdései

HADMÉRNÖK 13 : 3 pp. 9-17. , 9 p. (2018)

[K4] Gábor, Bréda; Security Challenges of Smart Meeting Rooms in Smart Cities

ÓBUDA UNIVERSITY E-BULLETIN 8 : 1 pp. 5-12. , 8 p. (2018)

[K5] Kiss, Miklos ; Breda, Gabor ; Muha, Lajos; Information security aspects of Industry 4.0

PROCEDIA MANUFACTURING 32 pp. 848-855. , 8 p. (2019)

[K6] Gábor, Bréda ; Péter, János Varga; Protected spaces in smart citiesandthe identification of new radio signalsin their environment usinga complexmeasurement method

INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS 17 : 1-A pp. 67-77. , 11 p. (2019)

[K7] Gábor, Bréda; Monitoring optical data connection between protected rooms in smart cities

INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS 17 : 3 pp. 444-457. , 14 p. (2019)

[K8] Breda, Gabor ; Kiss, Miklós; Overview of Information Security Standards in the Field of Special Protected Industry 4.0 Areas & Industrial Security

PROCEDIA MANUFACTURING 46 pp. 580-590. , 11 p. (2020)

Tudományos konferencia kiadvány, könyvrészlet közlemények:

[K9] Bréda, Gábor; Dóka, László; Varga, PéterJános;

The examination of the development of the communication devices on the commercial market In: Szakál, Anikó (szerk.) 17th IEEE International Symposium on Computational Intelligence and Informatics (CINTI 2016)

Budapest, Magyarország : IEEE Hungary Section (2016) 370 p. pp. 303-307. , 5 p.

[K10] Bréda, Gábor; Védett helyiségek biztonságának szempontjai - Safety acpects of protected areas

In: Rajnai, Zoltán (szerk.) Kiberbiztonság - Cyber Security : Tanulmánykötet a Biztonságtudományi Doktori Iskola kutatásaiból

Budapest, Magyarország : Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, (2018) pp. 185-198. , 14 p.

[K11] Gábor, Bréda ; Péter, János Varga ; Zsolt, Illési; Forensic Functional Profile of IoT Devices: Based on Common Criteria

In: Anikó, Szakál (szerk.) 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY) : Proceedings

Budapest, Magyarország : IEEE Hungary Section (2018) 344 p. pp. 261-264. , 4 p.

[K12] Bréda, Gábor; Designing a protected room from information security aspect, a personal approach

In: Rajnai, Zoltán (szerk.) Kiberbiztonság – Cybersecurity 2.

Budapest, Magyarország : Óbudai Egyetem, Biztonságtudományi Doktori iskola (2019) 247 p. pp. 147-154. , 8 p.

[K13] Gábor, Bréda; Design a Protected Room from Information Security Aspect, a Personal Approach

In: Rajnai, Zoltán; Schmidt, Péter; Jurik, Pavol (szerk.) Eight International Scientific Web-conference of Scientists and PhD. students or candidates

Budapest, Magyarország : Óbuda University (2020) 224 p. pp. 145-152. , 8 p.

[K14] Bréda, Gábor; A villamosenergia ellátás biztonságának növelése a meddő villamos energia kompenzációja révén

In: Rajnai, Zoltán (szerk.) Kiberbiztonság – Cybersecurity 2.

Budapest, Magyarország : Óbudai Egyetem, Biztonságtudományi Doktori iskola (2019) 247 p. pp. 30-46. , 17 p.

[K15] Bréda, Gábor; Védett helyiségek jelene és jövője

In: Rajnai, Zoltán; Fregán, Beatrix; Marosné, Kuna Zsuzsanna (szerk.) Tanulmánykötet a 7. BBK előadásaiból

Budapest, Magyarország : Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, (2016) pp. 677-682. , 6 p.

Szóbeli előadás és absztrakt kötetben megjelent közlemények:

[K16] Bréda, Gábor; Védett helyiségek és azok elhelyezése

In: Keresztes, Gábor (szerk.) Tavaszi Szél 2016 Konferencia. Nemzetközi Multidiszciplináris Konferencia : Absztraktkötet

Budapest, Magyarország : Doktoranduszok Országos Szövetsége (DOSZ) (2016) 485 p. pp. 303-303. , 1 p.

[K17] Bréda, Gábor; Védett helyiségek biztonságának szempontjai (2016)

X. Régiók a Kárpát-medencén innen és túl nemzetközi tudományos konferencia, Kaposvár, Kaposvári Egyetem, 2016 október 14.,

[K18] Bréda, Gábor; Az elhangzott szó védelme, védett tárgyaló, Protecting the spoken word, protected meeting room

In: Óbudai, Egyetem (szerk.) XXXIII. KANDÓ KONFERENCIA 2017: „Kandó a tudomány hajóján" Absztrakt kötet

Budapest, Magyarország : Óbudai Egyetem, (2017) pp. 31-32. , 2 p.

[K19] Bréda, Gábor; Okos város okos tárgyalóinak biztonsági kihívásai, The security challenges of smart meeting rooms in Smart Cities

In: Tokody, Dániel; Mgr. Ing. Gabriela Sopková, PhD. (szerk.) Smart City Konferencia 2017 Absztraktkötet : Smart City 2017 Conference Abstract Book

Budapest, Magyarország : Doktoranduszok Országos Szövetsége, (2017) p. 17 , 1 p.

[K20] Bréda, Gábor ; Varga, Péter János; Protected Spaces in Smart Cities and The Identification New Radio Signals in Their Environment Using a Complex Measurement Method

In: Tokody, Dániel; Tokodyné, Szabadi Nikolett (szerk.) Smart, Sustainable and Safe Cities Conference 2018 Abstract Book

Budapest, Magyarország : Doktoranduszok Országos Szövetsége (DOSZ) (2018) 40 p. pp. 30-30. , 1 p.

[K21] Kiss, Miklós ; Muha, Lajos ; Bréda, Gábor; Information Security Aspects of Industry 4.0 p. & (2018)

The 12th International Conference INTER-ENG 2018 Interdisciplinarity in Engineering, Konferencián elhangzott előadás,

[K22] Bréda, Gábor; Védett helyiségek információbiztonsága p. & (2018)

Doktoranduszok interdiszciplináris kutatásai a belügyi nemzetbiztonsági szférában, Előadás, Nemzeti Közszolgálati Egyetem,

[K23] Miklós, Kiss ; Gábor, Bréda; Overview of Information Security Standards in the Field of Special Protected Industry 4.0 Areas & Industrial Security (2019)

Szóbeli előadás, The 13th International Conference INTER-ENG 2019 Interdisciplinarity in Engineering, 3 - 4 October 2019, Târgu Mureș, Romania,

[K24] Gábor, Bréda; Designing a protected room from information security aspect, a personal approach (2020)

Trends and Innovations in E-business, Education and Security 2020, előadás a webkonferencián,

[K25] Bréda, Gábor; Védett helyiségek komplex biztonsága

In: Bárdos, Szabolcs (szerk.) Doktoranduszok Interdiszciplináris kutatásai a belügyi nemzetbiztonsági szférában

(2021) p. & , 1 p.

A KUTATÁSI EREDMÉNYEK FELHASZNÁLÁSA, AJÁNLÁSOK, JAVASLATOK

A kutatási eredményeimet az oktatás, a biztonságtudomány, az információ védelmi tevékenység kialakítása során, valamint a műszaki tudományok területén ajánlom hasznosítani, mivel az eredmények és azok struktúrája, tág horizontot teremt a témában. A téma feldolgozása során, több diszciplínához tartozó kérdéskör is beépítésre került, melynek eredményéül ok-okozati összefüggések kerültek párosításra a védett helyiség kialakításának érdekében, az ember-ember között létrehozott, közvetlen kommunikáció információtartalmának védelmére, a védett helyiség megvalósítását szem előtt tartva.

Az eredményeimet felhasználva a kutatás folyamán publikált ismeretek, képet adhatnak a szervezeti biztonság kialakításán dolgozó személyek képzési anyagának összeállításához, valamint választ adhatnak a döntéshozók biztonságtudatos kommunikációs környezet kialakítására vonatkozó kérdéseire. Az értekezésben képet kapunk az információ értékké alakulásának folyamatáról, amely során a figyelem a kommunikációs interaktus és annak értékteremtő folyamataira, valamint a kommunikáció biztonságának sebezhetőségére irányul.

Az értekezés eredményeinek felhasználását, ajánlom a biztonságos szervezeti struktúra technikai kialakításán dolgozó szakemberek számára, mivel a védett helyiségek kialakítása során, a kialakítani kívánt helyiség leírásával, a védett helyiség definíciója hasznos fogalom lehet a védett helyiségek egyértelmű azonosításának megfogalmazásával.

Az értekezést ajánlom nagy információs vagyonnal rendelkező szervezetek, intézmények biztonsági területekért felelős döntéshozói számára. Elemzés eredményei alapján és demonstratív úton is áttekintést adtam a témában megismerhető fenyegetettségeket összefoglalva, döntéstámogatói háttérismeretek növelése céljából. A kutatással elősegíthetem a védett helyiség szükséges kialakításának döntési relevanciáját, a szervezetekhez illesztve. Ajánlom a védett helyiség struktúra megvalósíthatóságának lehetőségét, valamint modellen keresztül konkrét megvalósítási javaslatot teszek „a védett helyiség" kialakítására.

A kutatás eredményeinek esetleges felhasználását javaslom a jogalkotó számára, biztonságos környezet kialakításának megteremtését célzó további szabályzó megfogalmazása céljából. A „Védett helyiség karbantartása, technikai átvizsgálása" című alfejezetében kifejtett gondolatok mentén elvégezhető technikai műveletek

esetleges implementálása, és azok lehetőség szerinti elvégzése, jelentős mértékben csökkentő hatást fejtenek ki a kommunikációs környezet maradványkockázatának mértékére.

Az innováció tekintetében, az elképzelt rádiós forrás lokalizáció eljárást hardverfejlesztéssel foglalkozó szervezetek figyelmébe ajánlom,a gyakorlati kialakítás céljából.

A kutatás optikai távközléssel foglalkozó részeit az oktatásban javaslom hasznosítani, a monitorozható fizikai réteg megismerése céljából.

Továbbá a munkám teljes terjedelmét mindazon érdeklődők számára ajánlom, akik érdeklődnek a téma iránt és átfogó képet kívánnak kapni e témában.

Javasolt további kutatási irány

A téma további javasolt kutatási irányait tekintve két irányt javaslok, melyek egyike a humán biztonságtudatosság megteremtését célzó irány, amely hozzájárul a biztonságos szervezet kialakításához. Valamint a másodikként a védett helyiségekben alkalmazható IT technikai berendezésekkel kapcsolatos hardver és szoftver kialakításának kutatási iránya, amely hozzájárulhat a védett helyiségekben alkalmazható IT technológiai berendezések biztonságának növeléséhez.

IRODALOMJEGYZÉK

[1] R. Lincoln Ackoff, „From Data To Wisdom," *Journal of Applies Systems Analysis 16,* %1. kötet16, pp. 3-9, 1989.

[2] M. Pollányi, The Tacit Dimension, New York: Dubleday and Company; Garden City, 1966.

[3] Z. Zoltayné Paprika, Döntéselmélet, Budapest: Aliena, 2005.

[4] G. Bellinger, D. Castro és A. Mils, „Data Information Knowledge and Wisdom," 2004. [Online]. Available: http://www.systems-thinking.org/dikw/dikw.htm.

[5] A. Dr Keszthelyi, Információbiztonság technikai alapismeretek, OEKGK Szervezési és Vezetési Intézet, Vállalkozásfejlesztés a XXI. században, Budapest, 2012.

[6] I. Nonaka és H. Takeuchi, The Knowledge creating Company: How Japanese Companies Create the Dynamics of Innovation, New York: Oxford University Press, 1995.

[7] L. Tóth és P. Szikora, „Data, Information, Knowledge in FUTÁR: Case Study of a Public Transportation Information System," *Science Journal of Business and Management,* %1. kötet3., %1. szám1-1., pp. 66-72., 2015.

[8] A. Miller George, „The magical number seven, plus or minus two: Some limits on our capacity for processing information.," *Psychological Review,* %1. szám63, pp. 81-97, 1956.

[9] S. March, A. Hevner és S. Ram, „Research Commentary: An Agenda for Information Technology Research in Heterogeneous and Distributed Environments," 2000. [Online]. Available: http://dx.doi.org/10.1287/ isre.11.4.327.11873. [Hozzáférés dátuma: 30. Nov 2014.].

[10] L. Muha, Fogalmak és definíciók, Budapest: Verlag Dashöfer Szakkiadó, 2002.

[11] L. S. Mátrail, „Üzleti hírszerzés, gazdasági (ipari) kémkedés 1. szám," *Terror & Elhárítás,* 2018.

[12] C. Gémes, „Az információbiztonság alapkérdései," *Hadmérnök XII. évfolyam 4- szám; Budapest,* pp. 128-137, 2017.

[13] E. Szűcs és L. Záhonyi, „Információbiztonság fejlődés-történeti vizsgálata-Mérföldkövek, események és válaszok,” *Biztonságtudományi Szemle 3:3,* pp. 81-91, 2021.

[14] Á. Vaszari, *Üzleti hírszerzés a multinacionális cégeknél és a kis és középvállalkozásoknál,* Budapest: Budapesti Gazdasági Főiskola Külkereskedelmi Főiskolai Kar, 2007.

[15] K. Lazányi, „A biztonsági kultúra szerepe a vezetői döntések ámogatásában; TAYLOR Gazdálkodás és szervezéstudományi folyóirat 2016. 1. szám Szeged p.143-150,” 2016. [Online]. Available: https://ojs.bibl.u-szeged.hu/index.php/taylor/article/view/12993/12849. [Hozzáférés dátuma: 10. június 2016].

[16] K. Lazányi, „A biztonsági kultúra, TAYLOR Gazdálkodás és szervezéstudományi folyóirat 2015. 1-2 szám, Szeged, p.398-405,” [Online]. Available: https://ojs.bibl.u-szeged.hu/index.php/taylor/article/view/12936/12792. [Hozzáférés dátuma: 07. december 2015].

[17] Z. Prof Dr Rajnai, „Információbiztonság tudatosság,” *XXII. Fiatal Műszakiak Tudományos Ülésszaka,Műszaki tudományos közlemények 7., Kolozsvár,* pp. 37-42., 2017.

[18] T. Farkas és E. Hronyecz, „Inokommunikációs szakemberek a védelmi szférában: Szakirányú továbbképzés,” *Műszaki Tudományos Közlemények (HU) 9:1,* pp. 75-78, 2018.

[19] I. Dobák, „Betekintés az állambiztonság 1960-70-es évei nemzetközi technikai kutatás-fejlesztési folyamatainak szerkezetébe,” *Hadmérnök: 8,* pp. 319-327, 2013.

[20] I. Dobák és I. Solti, „Az "operatív technika" fejlesztésének helye és szerepe az állambiztonság szervezetrendszerében - A szobalehallgatás,” *Hadmérnök 11:3,* pp. 121-134, 2016.

[21] *2012. évi C. törvény a Büntető Törvénykönyvről.*

[22] G. Fülöp, Az információ, Budapest: Eötvös Lóránd Tudományegyetem, 1996.

[23] C. Lavaud, R. Gerzaguet, M. Gautier, O. Berder, E. Nogues és S. Molton, „Whispering devices: A survey on how side-channels lead to compromised information,” HAL Science Ouverte, 21. Marc 2021. [Online]. Available: https://hal.archives-ouvertes.fr/hal-03176249. [Hozzáférés dátuma: May 2021].

[24] „US National Security Agency. Tempest: A signal problem," 1972.

[25] L. Pokorádi, „Technikai rendszerek megbízhatósága és biztonsága," *Szolnoki Tudományos Közlemények 2009:13,* 2009.

[26] *2013. évi V. törvény a Polgári Törvénykönyvről 2:46. § [A magántitokhoz való jog].*

[27] *2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.*

[28] *2009. évi CLV. törvény A minősített adat védelméről.*

[29] *2013. évi L. törvény Az állami és önkormányzati szervek elektronikus információbiztonságáról.*

[30] *41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról.*

[31] *26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáró.*

[32] *187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghat.ról.*

[33] *185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a bizt.ii események műszaki vizsg.nak és a sérülékenységvizsg.t lefolytat. szabról.*

[34] *161/2010. (V. 6.) Kormány rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól.*

[35] *92/2010. (III. 31.) Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairó.*

[36] *90/2010 (III.26.) Kormányrendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről.*

[37] *1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról.*

[38] *2018. évi LIV. törvény az üzleti titok védelméről.*

[39] *2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokró.*

[40] *2012. évi I. törvény A munka törvénykönyvéről.*

[41] P. Erdősi, *CISA Az üzleti hírszerzés és az ipari kémkedés ajánlás 2. változat,* Budapest: Budapesti Műszaki és Gazdaságtudományi Egyetem Gazdaság- és Társadalomtudományi Kar Információ- és Tudásmenedzsment Tanszék, 2005.

[42] „Cégvezetés Az üzleti titok védelme 55.szám," 01. november 2002. [Online]. Available: https://cegvezetes.hu/2002/11/az-uzleti-titok-vedelme/. [Hozzáférés dátuma: 14 Nov 2014].

[43] L. Muha és C. Krasznay, Az elektronikus Információs rendszerek menedzselése, KÖFOP-2.1.1-VEKOP-15-2016-00001 szerk., Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[44] J. Kerekes, L. Stampok, J. Tímár, Z. Tamás, B. Dr. Tóth, B. Nagy és S. Nyilas, Információ - Biztonság, Budapest: Cedit Információtechnikai Kft., 1997.

[45] L. Megyeri és T. Farkas, „Kockázatkezelés,tudomány vagy kurázsi," *Hadmérnök 12:3,* pp. 198-209, 2017.

[46] T. Berek és I. Elek, „Zárszerkezet, mint a mechanikai védelem sebezhető pontja," *Műszaki Katonai Közlöny 25:3,* pp. 47-58, 2015.

[47] S. Gyányi és L. A. Keszthelyi, Technológiai ismeretek, Budapest: NKE, 2014.

[48] Z. Haig és L. Kovács, Kritikus infrastruktúrák és kritikus információs infrastruktúrák Tanulmány TÁMOP 4.2.2/B-10/1-2010-0001, Budapest: Nemzeti Közszolgálati Egyetem, 2012.

[49] „Critical Foundations Protecting America's Infrastructures The Report of the President's Commissionon Critical Infrastructure Protection," Washington, 1997.

[50] B. Dr. Bognár, T. Dr. Bonnyai, D. G. Katalin, D. K.-U. Lajos és G. Dr. Vass, Létfontosságú rendszerek és létesítmények védelme, Budapest: Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézet, 2015..

[51] *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.*

[52] „EUR-Lex; Az Europai Parlament és Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységes magas szintjét biztosító intézkedésekről," 06 Jun 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L1148&from=en. [Hozzáférés dátuma: 05 January 2017].

[53] P. J. Varga, „Kritikus infrastruktúrák hatás alapú modellezése," *Hadmérnök 4:4,* pp. 390-399, 2009.

[54] J. P. Varga, „A kritikus információs infrastruktúrák értelmezése," *Hadmérnök III. évfolyam,* %1. szám 2., pp. 149-156., 2008.

[55] Z. Précsényi és J. Solymosi, „Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé,"Hadmérnök II.Évfolyam 1.szám," pp. 65-76, 2007.

[56] T. Kovács és A. Pallagi, „Kritikus infrastruktúrák komplex biztonságvédelmi rendszereinek tervezése, kialakítása, különös tekintettel a beléptetőrendszerek alkalmazására," *Hadmérnök 14:4,* pp. 35-45, 2019.

[57] G. Bréda és B. Hajdu, „A társadalom és a védett helyiségek kapcsolata, valamint a védett helyiségek kialakításához kapcsolódó tudományterületek," *KÖZTES EURÓPA: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI 9 : 1-2 pp. 89-96. , 8 p.,* 2017.

[58] E. Szűcs és M. Szakali, „A biztonság ára, avagy a védelmi költségvetés emelkedésének lehetséges hatásai," *Hadmérnök 13:1,* pp. 314-325, 2018.

[59] H. Szabó és I. Dobák, „Az információs társadalom nemzetbiztonsága," *Nemzet és Biztonság:Biztonságpolitikai szemle 14 : 2 ,* pp. 93-110, 2021.

[60] S. Steven, „The People, Policy, Technology (PPT) Model: Core," [Online]. Available: https://ur.booksc.eu/book/51467443/0a5c17. [Hozzáférés dátuma: 14 március 2020].

[61] L. Berek, Biztonságtechnika ÁROP – 2.2.21, Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[62] B. Boros, R. Bottyán, S. Dessewffy, I. Koskovics, J. Kovács, F. Liszt, L. Móró és L. dr. Szili, Rendészet, vagyonvédelem, Budapest: Buapesti Műszaki Egyetem Mérnöktovábbképző Intézet, 1997.

[63] R. Pető, „Épületvédelem metódusa robbantásos cselekmények ellen," *Műszaki Katonai Közlöny 23:1 ISSN 2063-4986,* pp. 51-58, 2013.

[64] L. Dr. Berek, T. Dr. Berek és L. Berek, in *Személy és vagyonbiztonság*, Budapest, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2016, p. 32.

[65] A. Őszi, „Az e-kereskedelem elvárásai a biometriával szemben," in *Vállalkozásfejlesztés a XXI. században: IV. tanulmánykötet*, Nagy Imre Zoltán, Szerk., Budapest, Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2014, pp. 427-440.

[66] G. Lukács, A. Dőring és P. Hell, Vagyonvédelmi rendszerek I., Budapest: Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar, 2015.

[67] A. Dőring, P. Hell és G. Dr. Lukács, Analóg áramkörök és érzékelők II., Budapest: Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar, 2015.

[68] Á. Guttengeber, L. Szili, F. Cserhalmi, G. Szűcs, L. Móró és B. K. Dunai, *Személy és vagyonőrök, biztonságtechnikai szakemberek tankönyve,* Budapest: Pro-Sec Kft..

[69] Z. Kuris, „A komplex információvédelem új irányai a nemzeti minősített adatok védelmével összefüggésben," *Hadmérnök V. évfolyam 4. szám; Budapest,* 2010.

[70] MABISZ, „Betöréses lopás- és rablásbiztosítás technikai feltételei (Ajánlás)," 12 február 2021. [Online]. Available: http://www.pluto.hu/_A/A2.html. [Hozzáférés dátuma: június 2021].

[71] Z. Prof Dr Rajnai, „Kritikus infrastruktúrák védelme," *XXI. Fiatal Műszakiak Tudományos Ülésszaka,Műszaki tudományos közlemények 5., Kolozsvár,* pp. 349-352., 2016.

[72] P. Vadász, „Információkeresés a gazdasági hírszerzésben; Hadmérnök IX: évfolyam 2. szám," *Budapest,* 2014.

[73] Dobák és Imre, „Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében: Hadmérnök 12," pp. 235-249, 2017.

[74] J. Dr. Boda és I. Dr. Dobák, A nemzetbiztonság technikai kihívásai a 21. században, Budapest: Nemzeti Közszolgálati Egyetem Szolgáltató Nonprofit Kft., 2015.

[75] T. Wührl, G. Lukács és G. Mágel, Híradástechnika I., Budapest: Bidapesti Műszaki Főiskola Kandó Kálmán Villamosmérnöki Kar, 2008, p. 174.

[76] G. Lukács és T. Wührl, Híradástechnika I., Budapest: Óbudai Egyetem, 2012, p. 225.

[77] S. Forgo, „Shannon és Weaver információelmélet (híradástechnikai) modellje," [Online]. Available: https://forgos.uni-eszterhazy.hu/wp-content/tananyagok/tarsesmedkomm_pc_exe/415_shannon_s_weaver_informcielmleti_hradstechnikai_modellje.html.

[78] S. Forgó, „Tanulás és az új médiumok TÁMOP-4.1.2-A/1-11/1-2011-0021," in *Shannon és Weaver információelméleti (híradástechnikai) modellje*, Eger, Eszterházy Károly Főiskola, 2013.

[79] A. S. Tanenbaum és D. J. Wetherall, Számítógép hálózatok, Budapest: Taramix Kft., 2013.

[80] F. A. Everest, Masters Handbook of Acoustics Fourth Edition, USA: McGraw-Hill Companies, Inc., 2001.

[81] T. Dr. Tarnóczy, Akusztikai Tervezés, Budapest: Műszaki Könyvkiadó, 1966.

[82] J. P. Nagy, A hangszigetelés elmélete és gyakorlata, Budapest: Akadémiai kiadó, 2004.

[83] „Paroc Sound insulation," 2019. [Online]. Available: https://www.paroc.pl/knowhow/sound/sound-insulation?sc_lang=en. [Hozzáférés dátuma: Marc 2021].

[84] F. Agusztinovicz, „Hangterjedés akadályozott terekben; Mérnöki Akusztika oktatási segédlet," 2014. [Online]. Available:

https://last.hit.bme.hu/download/fulop/MernokiAkusztika_14/Hangelnyel%c3%a9s-g%c3%a1tl%c3%a1s_MAkusz.pdf. [Hozzáférés dátuma: május 2020].

[85] Z. Varga, „Hang és halláskárosodás," 10. március 2019. [Online]. Available: https://www.fuldugo.hu/hirek/aktualis/hang-es-hallaskarosodas. [Hozzáférés dátuma: február 2021].

[86] B. Collings, G. Lietaert és F. Heismann, Reference Guide to Fiber Optic Testing Volume 2; JDSU Corporation, 2010.

[87] H. Tanaka, O. Takizawa és A. Yamamura, „A Trial of the Interception of Display Image using Emanation of Electromagnetic Wave," Journal of the National Institute of Information and Communications Technology Vol.52, 2005, pp. 213-223.

[88] NBF, „A TEMPEST-ről és a kompromittáló elektromágneses kisugárzás elleni védelem eszközeiről," [Online]. Available: https://www.nbf.hu/hasznos-informaciok/tempest/. [Hozzáférés dátuma: január 2017].

[89] M. G. Kuhn, „Electromagnetic eavesdropping risks of flat-panel displays," Privacy Enhancing Technologies, Springer, 2005.

[90] W. V. Eck, „Electromagnetic radiation from video display units: an eavesdropping risk?," *Computers and Security 4.,* pp. 169-286, 1985.

[91] M. G. Kuhn, „Compromising emanations of lcd tv sets.," Electromagnetic Compatibility (EMC), 2011 IEEE International Symposium IEEE, 2011, pp. 931-936.

[92] M. G. Kuhn, Compromising emanations:eavesdropping risks of computer;, University of Cambridge Computer Laboratory, 2003.

[93] I. Kubiak, „Laser printer as a source of sensitive emission," *Turkish Journal of Electrical Engineering & Computer Sciences,* %1. kötet26., pp. 1354-1366, 2018.

[94] M. Marinov, „Remote video eavesdropping using a software-defined radio platform; Doctoral Dissertation," 11 Jun 2014. [Online]. Available: https://github.com/martinmarinov/TempestSDR/blob/master/documentation/acs-dissertation.pdf. [Hozzáférés dátuma: Okt 2020].

[95] M. Marinov, „TempestSDR program," 14. Apr 2020. [Online]. Available: https://github.com/martinmarinov/TempestSDR/tree/master/TempestSDR. [Hozzáférés dátuma: Okt 2020].

[96] „Advanced Electronic Security Co.," [Online]. Available: www.bugsweeps.com/info/spytech.html. [Hozzáférés dátuma: Febr 2019].

[97] „TIME, ELECTRONICS Bug Thy Neighbo, pp.55-56," 06. March 1964. [Online]. Available: https://time.com/vault/issue/1964-03-06/page/61/. [Hozzáférés dátuma: Jul 2019].

[98] I. dr. Solti, A titkos információgyűjtés, elvei, eszközei és módszerei, alkalmazásának lehetőségei a nemzetbiztonsági munkában Doktori (PhD) értekezés, Budapest: Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, 2017.

[99] T. Johnes, „3rd International Security Symposium - TSCM - Modern Eavesdropping Threats Presentation," October 2020. [Online]. Available: https://www.youtube.com/watch?v=KFrZ6SPMZNo. [Hozzáférés dátuma: Dec 2020].

[100] I. Dr. Töltési, „Lehallgatásvédelem az üzleti szférában 1.," *Detektor plusz,* %1. szám7., pp. 32-33, július 2006..

[101] I. Dr. Töltési, „Lehallgatásvédelem az üzleti szférában 2.," *Detektor plusz,* pp. 58-59, augusztus-szeptember 2006.

[102] I. Dr. Töltési, „Lehallgatásvédelem az üzleti szférában 3.," *Detektor plusz,* pp. 47-49, október-november 2006.

[103] „Special Report DIGITAL 2021," [Online]. Available: https://wearesocial.com/uk/blog/2021/01/digital-2021-uk/. [Hozzáférés dátuma: Nov 2021].

[104] T. Berek, „Okos rendszerek lehetőségei és biztonsági kihívásai," *Biztonságtudományi Szemle 1:1-2,* pp. 7-16, 2019.

[105] „CICS - Center for Strategic and Internetional Studies, Significant Cyber Incidents Since 2006 - 2021," 05. Nov 2021. [Online]. Available: https://csis-website-prod.s3.amazonaws.com/s3fs-public/211105_SignificantCyberIncidents.pdf?_Bux.NVhaioSPTAcspLrKuLx.xCZNSP3. [Hozzáférés dátuma: Dec 2021].

[106] „Global Security Mag, Significant cyber attacks 2006 May - 2020 June," Jul 2020. [Online]. [Hozzáférés dátuma: Marc 2021].

[107] P. J. Varga, „Az okos otthonok vezeték nélküli alkotóelemeinek biztonsága," *Köztes Európa: Társadalomtudományi Folyóirat: A VIKEK Közleményei 9:1 ,* pp. 83-87, 2017.

[108] L. Ványa, „Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre," in *Doktori értekezés*, Zrínyi Miklós Nemzetvédelmi Egyetem, 2001.

[109] Z. Haig, „Az információbiztonság komplex értelmezése," *Hadmérnök, Robothadviselés 6.,* %1. kötetKülönszám, p. 9., 2006.

[110] A. Kerti, A vezetési és információs rendszerek technikai alrendszerének vizsgálata különös tekintettel a minőségbiztosításra és az átvitelbiztonságre Doktori értekezés, Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola, 2010.

[111] Z. Haig, „Az információs társadalmat fenyegető információalapú veszélyforrások," *Hadtudomány XVII. évfolyam 3. szám,* Sept 2007.

[112] L. Muha, A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, Doktori értekezés, Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2007.

[113] L. Muha és Á. Bodlaki, Az informatikai biztonság, Budapest: PRO-SEC KFT, 2007.

[114] M. Környei, „Üzleti titok védelme," *Pécsi Tudományegyetem Óriás Nándor Szakkollégium, Scriptura Folyóirat I. kötet,* pp. 170-185., 2015.

[115] Z. Kuris, „Komplex információbiztonság megvalósítási lehetőségeinek megközelítésa," *Hadmérnök II. évfolyam 1. szám,* pp. 311-318, 2009.

[116] S. Bulja, R. Kopf, T. A és T. Hu, „High Frequency Dielectric Characteristics of Electrochromic WO3 and NiO Films with LiNbO3 Electrolyte," *Scientific Reports,* %1. kötet DOI: 10.1038/srep28839, p. 6:28839 |, 30 June 2016.

[117] „FORTUNE," [Online]. Available: https://fortune.com/2015/10/28/smart-windows/. [Hozzáférés dátuma: April 2021].

[118] S. d. o. s. insulation, „https://www.designingbuildings.co.uk/wiki/Sound_insulation_in_buildings," [Online].

[119] K. h. s. hatása, „https://www.rigips.hu/hu/epuletakusztika," [Online]. Available: https://www.rigips.hu/hu/epuletakusztika. [Hozzáférés dátuma: november 2019].

[120] F. Augusztinovicz, „A beszéd, Segédlet," [Online]. Available: https://last.hit.bme.hu/download/kommtech/5_Beszed.pptx.

[121] B. Berglund és T. Lindvall, „Community Noise," [Online]. Available: https://www.nonoise.org/library/whonoise/whonoise.htm. [Hozzáférés dátuma: may 2020].

[122] H. Flechter és R. H. Galt, „The Preception os Speech and Its Relation to Telephony," *The Journal of the Acustical Society of America,* %1. kötetVol22 Number 2, 1950 march.

[123] T. Tarnóczy, „A beszédérthetőség mint fizikai fogalom," Fizikai Szemle, 1995 marc. [Online]. Available: http://fizikaiszemle.hu/archivum/fsz9503/tarn9503.html#ir. [Hozzáférés dátuma: marc 2020].

[124] G. Dr. Wersényi, „Telekommunikácio 2," Széchenyi István Egyetem Távközlési Tanszék , 2022. [Online]. Available: http://vip.tilb.sze.hu/~wersenyi/TK2_J.pdf. [Hozzáférés dátuma: jan 2022].

[125] „reiusa.net," REI, [Online]. Available: https://reiusa.net/wp-content/uploads/2017/11/ANG_Manual_revG.pdf. [Hozzáférés dátuma: marc 2020].

[126] L. H. Hemming, Architectural Electromagnetic Shielding Handbook, New York: The Institute of Electronics Engineers, Inc. IEEE Press, 1992.

[127] „ResearchGate EM field," [Online]. Available: https://www.researchgate.net/figure/An-EM-wave-consists-of-2-components-electric-field-and-magnetic-field-oscillating-in_fig8_280872394. [Hozzáférés dátuma: maj 2021].

[128] „Electronics Notes EMI coupling mechanism," [Online]. Available: https://www.electronics-notes.com/articles/analogue_circuits/emc-emi-electromagnetic-interference-compatibility/what-is-emi-basics-tutorial.php.

[129] „IEEE-STD299-2006," [Online]. Available: https://www.lisungroup.com/wp-content/uploads/2020/02/IEEE-STD299-2006-Standard-Free-Download.pdf. [Hozzáférés dátuma: április 2021].

[130] „MSZ EN 50147-1:1988," [Online]. Available: http://www.mszt.hu/web/guest/webaruhaz;jsessionid=F5C2352939D449A1BBFBA4F8987EC92D?p_p_id=msztwebshop_WAR_MsztWAportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_msztwebshop_WAR_MsztWAportlet_ref=068379&_msztwebsh. [Hozzáférés dátuma: marc 2021].

[131] „Holland Shielding Fólia és textil árnyékoló anyagok," [Online]. Available: https://hollandshielding.com/Mu-copper-foil. [Hozzáférés dátuma: February 2022].

[132] „EM shield Árnyékolt szoba," EM shield, [Online]. Available: https://emshield.de/en/portfolio/radiation-protection-tempest/. [Hozzáférés dátuma: április 2021].

[133] „S101 panel attenuation line," [Online]. Available: https://www.ets-lindgren.com/products/shielding/rf-shielding-and-accessories/11003/1100312?page=Products-Item-Page. [Hozzáférés dátuma: mac 2021].

[134] „RFD-60 árnyékoló ajtó," [Online]. Available: https://www.ets-lindgren.com/products/shielding/rf-shielding-and-accessories/11004/1100410?page=Products-Item-Page. [Hozzáférés dátuma: may 2021].

[135] „Hollandshielding Nagyteljesítményű szűrő," [Online]. Available: https://hu.hollandshielding.com/Ultra-nagy-teljes%C3%ADtm%C3%A9ny%C5%B1-sz%C5%B1r%C5%91k-a-legmagasabb-%C3%A1rny%C3%A9kol%C3%A1si-ig%C3%A9nyekhez-8010. [Hozzáférés dátuma: Jan 202].

[136] „Hollandshield Árnyékolt szellőző átvezető," [Online]. Available: https://hu.hollandshielding.com/Honeycomb-szell%C5%91z%C5%91-panelek. [Hozzáférés dátuma: February 2022].

[137] „Canadian Centre for Cyber Security; teria for the Design, Fabrication, Supply, Installation and Acceptance Testing of Walk-in, Radio-Frequency-Shielded Enclosures (ITSG-02),"

[Online]. Available: https://cyber.gc.ca/sites/default/files/publications/itsg-02-eng.pdf. [Hozzáférés dátuma: February 2022].

[138] „MIL-HDBK-1195," [Online]. Available: http://www.tscm.com/MIL-STD-1195.pdf. [Hozzáférés dátuma: January 2022].

[139] „MIL-STD-461E; Department of Defense Interface Standard," [Online]. Available: http://www.chassis-plans.com/PDF/MIL-STD-461E.pdf. [Hozzáférés dátuma: 06 January 2018].

[140] K. E. Németh és T. Gregász, „Development of Measurement Method for Testing the Shielding Properties of Textiles andAnalysis of Avialibity of the Measurment System," *Óbuda University e-Bulletin,* %1. kötet2, %1. szám1, pp. 201-215, 2011.

[141] „2003. évi C. törvény Az elektronikus hírközlésről," [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a0300100.tv.

[142] „7/2015.(XI.13) NMHH rendelet," [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1500007.nmh. [Hozzáférés dátuma: Marc 2021].

[143] „2/2017. (I. 17.) NMHH rendelet a rádióberendezésekről," [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1700002.nmh. [Hozzáférés dátuma: March 2021].

[144] G. Bréda, Optikai szálfelügyeleti rendszer tervezése; Diplomamunka, Budapest: Óbudai Egyetem, 2014.

[145] T. Wührl és S. Gyányi, Számitógéphálózati alapismeretek, Budapest: MATÁV Kotatási Központ, 2006, p. 100.

[146] L. Choquet, „Reference Guide to Fiber Optic Testing Glossary," *JDSU Corporation,* 2008.

[147] J. Larerriée, G. Lietaert, R. Taws és S. Wolszczak, Reference Guide to Fiber Optic Testing Volume 1; JDSU Corporation, 2007.

[148] „Small Bandwith OTDR (Optical Time Reflectometer) for reflection measurement of DWDM systems used in the Antares project Pieter N.J.M. Jansen rt al.," January 2004. [Online]. Available: http://www.nikhef.nl/~jelle/antareswebdocuments/Sb_otdr/SB-OTDR.pdf. [Hozzáférés dátuma: May 2018].

[149] NTest Fiber Watch RFTS System-0904, 2008.

[150] „Fiber Optic Cable Tutorial," [Online]. Available: http://www.fiberoptics4sale.com/Merchant2/fiber-optic-cable.php. [Hozzáférés dátuma: March 2008].

[151] M. Mary, S. P. Varghese, M. Swarish és S. Nair, „A novel real time Remote Fiber Monitoring System," Ne ST Research & Development Centre, Plot43; CSEZ; Coshin India, [Online]. Available: http://een.iust.ac.ir/profs/Sadr/Papers/netp9.pdf.

[152] Z. Végvári, „A lehallgatás ellen védett mobiltelefonálás összehasonlító vizsgálata, Katonai logisztika 22. évfolyam 2. szám," pp. 146-170, 2014.

[153] P. Vizi, „Okostelefonok biztonsági kihívásai," Hadmérnök VI. évfolyam 3. szám. Sept 2011.," pp. 131-141.

[154] Z. Haig és I. Várhegyi, Hadviselés az információs hadszíntéren, Budapest: HM Zrínyi Kommunikációs Kht, 2005.

[155] *MSZ 27001:2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények.*

[156] G. Schuster és G. Terpecz, „Kritikus sikertényezők vagy elkerülhetetlen veszélyforrások," *Szolnoki Tudományos Közlemének 16: különszám,* pp. 347-363, 2012.

[157] „156/2017. (VI. 16.) Korm. rendelet a haditechnikai tevékenység engedélyezésének és a vállalkozások tanúsításának részletes szabályairól," [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1700156.kor. [Hozzáférés dátuma: January 2021].

[158] „Granite Island Group Technical Sourveillance Counter Measures," [Online]. Available: http://www.tscm.com/TSCMSequence.html. [Hozzáférés dátuma: January 2021].

[159] R. Sasvár, *Üzleti hírszerzés,* Budapest: Grafika Press Rt., 2006.

[160] „MURRAY ASSOCIATES TSCM Inspection Process," [Online]. Available: https://counterespionage.com/tscm-inspection-process/. [Hozzáférés dátuma: January 2021].

[161] „Implementing TSCM Sweeps for Business," [Online]. Available: https://execsecurity.com/wp-content/uploads/2018/10/Implementing-TSCM-for-Corporations.pdf. [Hozzáférés dátuma: January 2021].

[162] „Technical Surveillance Countermeasures," [Online]. Available: https://www.energy.gov/sites/default/files/2020/07/f76/HQFMSP-Chapter-9-Technical-Surveillance-Countermeasures-Feb-2018.pdf. [Hozzáférés dátuma: January 2021].

[163] „PURCHASING TSCM EQUIPMENT; INTERNATIONAL INTELLIGENCE LIMITED," [Online]. Available: https://www.international-intelligence.co.uk/purchase-tscm-equipment.html. [Hozzáférés dátuma: January 2021].

[164] „SHEARWATER TSCM; PRODUCT," [Online]. Available: https://shearwatertscm.com/products/. [Hozzáférés dátuma: January 2021].

[165] P. T. Wolf, Lehallgatás technika, Budapest: Marktech Kft., 1990.

[166] „TSCM – Technical Surveillance Counter Measures-CRFS," [Online]. Available: https://www.crfs.com/tscm. [Hozzáférés dátuma: March 2021].

[167] „Radio Inspector," [Online]. Available: https://radioinspector.com/. [Hozzáférés dátuma: February 2021].

[168] „Kestrel TSCM," [Online]. Available: https://kestreltscm.com/. [Hozzáférés dátuma: February 2021].

[169] „Wireless activity monitor," [Online]. Available: https://www.amazon.co.uk/Wireless-activity-JJN-WAM-108T-independent/dp/B0792BRZW2. [Hozzáférés dátuma: April 2021].

[170] K. Rothammel, Antennakönyv, Budapest: Műszaki könyvkiadó, 1977.

[171] Z. Németh, Helymeghatározás vezeték nélküli hálózatokon, Budapest: BME Méréstechnikai és Információs Rendszerek Tanszék; Szakdogozat, 2009. május 04.

[172] „Lokalizáxiós módszerek, protokollok és alkalmazhatóságuk," GOP 1.1.1-11-2011-0048 Tanulmánykötet; Használatalapú Díjfizatést lehetővé tévő hulladékgyűjtési rendszerek, [Online]. Available:

http://www.corvex.hu/files/3214/2668/9380/R14AB_Lokalizacios_modszerek_protokollok_es_alkalmazhatosaguk.pdf. [Hozzáférés dátuma: 05 January 2018].

[173] P. Denisowsky, „An Introduction to Radio Direction Finding Methodologies," [Online]. Available: https://wireless.vt.edu/symposiumarchives/2015_slides/document.pdf. [Hozzáférés dátuma: 05 January 2018].

[174] R. A. Nisar, „Radio Direction Finding Theory and practices," [Online]. Available: https://www.researchgate.net/profile/Nisar_Ahmed10/publication/289779492_Radio_Direction_Finding_Theory_and_Practices/links/569e752508ae21a56424b5a2/Radio-Direction-Finding-Theory-and-Practices.pdf. [Hozzáférés dátuma: 05 January 2018].

[175] G. Takács, „Helymeghatározás mobiltelefonnal LXIII. évf.2008/8," pp. 20-27..

[176] „International Telecommunication Union: Recommendation ITU-R P-1238-7: Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 900 MHz to 100 GHz," [Online]. Available: https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.1238-7-201202-S!!PDF-E.pdf. [Hozzáférés dátuma: 05 January 2008].

[177] T. Wührl, „GPS navigációs problémák UAV alkalmazásokba, Hadmérnök:Különszám," p. 8, 2006.

[178] K. Gyöngyösi, J. P. Varga és Z. Illési, „WLAN heat mapping in hybrid network," *INFORMATICS 2017; IEEE 14th International Scientific Conference on Informatics Proceedings.(ISBN:978-1-5386-0888-3),* p. 437., 2017.

[179] „A Sort Tutorial on Inertial Navigation System and Global Positioning System Integration," [Online]. Available: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20150018921.pdf. [Hozzáférés dátuma: 20 January 2018].

[180] O. J. Woodman, „An introduction to inertial navigation,," Technical Report University of Cambridge, Computer Laboratory, Number 696, ISSN 1476-2986, 2018. [Online]. Available: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-696.pdf. [Hozzáférés dátuma: 05 January 2018].

[181] „NLJD kapu," [Online]. Available: https://safrex.net/product-showcase/technical-surveillance-counter-surveillance/. [Hozzáférés dátuma: 10 Nov 2021].

[182] „Test szkenner," [Online]. Available: https://www.google.com/imgres?imgurl=https%3A%2F%2Fimages.radio.com%2Faiu-media%2Fdupage-county-jail-scanner-1fe96d0f-e304-40a6-b28a-0b8f6427d7f3.jpg&imgrefurl=https%3A%2F%2Fwww.audacy.com%2Fwbbm780%2Farticles%2Fdupage-county-sheriff-purchases-scanning-ma. [Hozzáférés dátuma: 10 Nov 2021].

[183] „Test szkenner 2," Adany Systems, [Online]. Available: https://www.police1.com/police-products/technology/body-scanners/articles/getting-the-most-from-your-body-scanner-23Cbbm8DZdPigOkK/. [Hozzáférés dátuma: 10 Nov 2021].

[184] „Csomagröntgen 3," [Online]. Available: https://znz.hu/termekek/rontgenberendezesek/. [Hozzáférés dátuma: 10 Nov 2021].

[185] „Csomagröntgen 2," [Online]. Available: https://hu.pinterest.com/pin/562105597222449972/. [Hozzáférés dátuma: 10 Nov 2021].

[186] „Csomagrontgen," [Online]. Available: https://www.gettyimages.com/detail/photo/x-ray-image-of-a-briefcase-carrying-a-mobile-phone-royalty-free-image/57339916. [Hozzáférés dátuma: 10 Nov 2021].

[187] I. P. Antók, Fényvezető hálózatok II. Fényvezető Hálózat alapismeret, Budaoest, 2011.

[188] I. P. Antók, Fényvezető hálózatok VI.; Fényvezető hálózatok létesítése II., Budapest, 2011.

[189] L. Cebe, Fénytávközlés I., Budapest: Kandó Kálmán Műszaki Főiskola, 1990.

[190] L. Smigura, Távközlő kábelek és vezetékek, Budapest: Magyar Posta Könyvkiadó, 1989.

[191] I. P. Antók, Fényvezető Hálózatok VIII., Fényvezető hálózatok tervezése II., 2011., Budapest.

[192] I. P. Antók, Fényvezető hálózatok IX., Szélessávú Optikai Hálózat Tervezése; 2011., Budapest.

[193] I. Jutasi, P. Vámos, E. Márkus, K. dr. Tamay és G. Nádorfi, Fényvezető távközlési rendszer tervezése (CCITT), Budapest: Távközlési Könyvkiadó, 1991.

[194] A. dr. Gyárfás, Optikai elemek mérése EDUCOPTIC mérőberendezéssel, Budapest: Budapesti Műszaki Főiskola; Kandó Kálmán Villamosmérnöki Főiskolai Kar, 2006.

[195] A. dr. Gyárfás, Optikai szálak mérése OTDR-rel, Budapest: Kandó Kálmán Műszaki Főiskola, 1997.

[196] G. Lajtha, Fénytávközlő rendszerek és elemeik, Budapest: Akadémiai Kiadó, 1987.

[197] G. Ákos, P. Jani, S. Varró, L. Andor és J. Balázs, Lézerek tudományos és gyakorlati alkalmazása; Fényvezető szálak és fénytávközlés, Prosperitas Kft. nyomda, 1993.

[198] I. P. Antók, Fényvezető kábelhálózat építése;, Mackensen Kft. nyomba, 2008.

[199] I. P. Antók, Fényvezető Hálózatok Gyakorlat, Passzív és aktív elemek a gyakorlatban 2., Budakalász, 2011.

[200] A. Elek, Nyomvonalas hálózatépítési technológiák kézikönyve, Budapest: Magyar Elektrotechnikai és Infokommunikációs Szövetség, 2006.

[201] „TIA/EIA STANDARD; Commercial Building Telecommunications Cabling Standard; APRIL 12. 2001," [Online]. Available: http://www.nag.ru/goodies/tia/TIA-EIA-568-B.1.pdf. [Hozzáférés dátuma: Marc 2018].

[202] „Live Fiber Monitoring in CWDM Network Part2," [Online]. Available: http://www.exfo.com/corporate/blog/2010/live-fiber-monitoring-cwdm-networks-part-2. [Hozzáférés dátuma: September 2018].

[203] „3M™ Planar Light Circuit (PLC) Optical Splitters," [Online]. Available: http://multimedia.3m.com/mws/mediawebserver?66666UuZjcFSLXTtmxfcOXM6EVuQEcuZgVs6EVs6E666666--. [Hozzáférés dátuma: October 2018].

[204] „Active Fiber Monitoring," [Online]. Available: http://www.ntestinc.com/activefiber.html. [Hozzáférés dátuma: September 2018].

[205] „Optikai Kábelek; Sommerkábel 2011.05," [Online]. Available: http://www.sommerkabel.hu/optikai-kabelek-leiras.html. [Hozzáférés dátuma: Oktober 2018].

[206] „Dark Fiber Monitoring; NTEST," [Online]. Available: http://www.ntestinc.com/darkfiber.html. [Hozzáférés dátuma: Oktober 2018].

[207] „Live Fiber Monitoring in CWDM Networks, Olivier Plomteux, Senior Product Line Manager, Optical Business Unit," [Online]. Available: http://www.ccontrols.ch/cms/upload/downloads/Telecom/1206EN_FiberGuardianAplicationNoteLiveFiberMonitoringCWDM.pdf. [Hozzáférés dátuma: September 2018].

[208] D. Kozischek és M. Bolick, „Planning Link-Loss Budgets Using Statistics; Broadband Propertier; June 2007.," [Online]. Available: http://www.broadbandproperties.com/2007issues/jun07issues/corning_june.pdf. [Hozzáférés dátuma: July 2018].

[209] „Light Amplifiers;," [Online]. Available: http://ftp.utcluj.ro/pub/users/cemil/dwdm/dwdm_Intro/8_5311715.pdf. [Hozzáférés dátuma: March 2018].

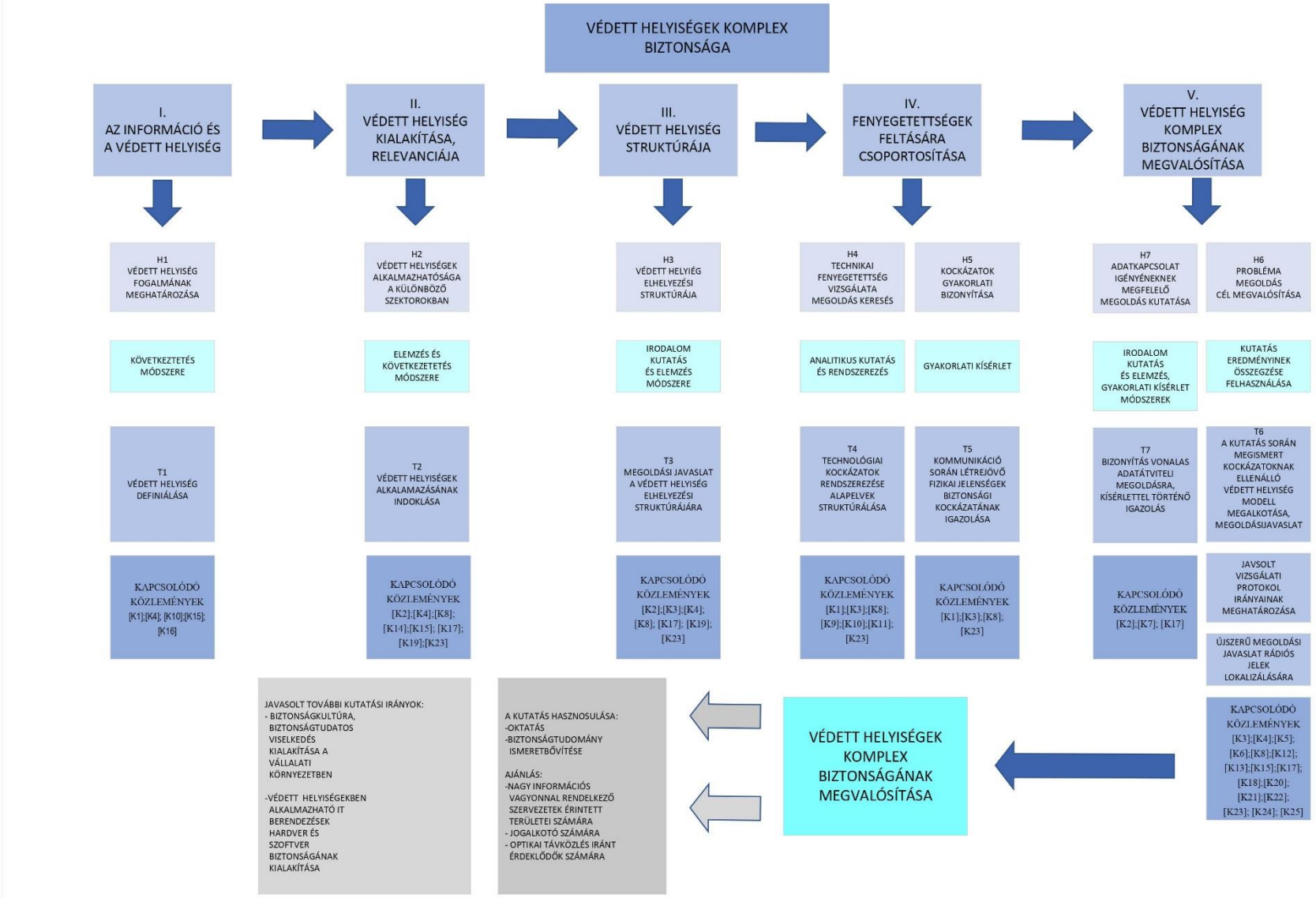
[210] „Fiber Optic Cable;," [Online]. Available: http://www.lanshack.com/fiber-optic-tutorial-cable.aspx. [Hozzáférés dátuma: October 2018].

[211] „Fibre Formulas made simple," [Online]. Available: http://www.tripleplay.co.za/uploads/Optical%20Fibre%20Formulas.pdf. [Hozzáférés dátuma: September 2018].

ÁBRAJEGYZÉK

TÁBLÁZATJEGYZÉK

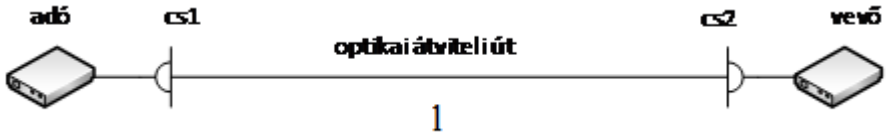
1.SZÁMÚ MELLÉKLET A KUTATÁS TÉRKÉPE



2. SZÁMÚ MELLÉKLET

Optikai szálkapcsolat csillapításának mérési elve, valamint optikai szálak OTDR-el (optical time-domain reflectometer) történő monitorozása

Az optikai szálakat különböző paramétereik szerint minősítik, amelyek nagyon fontosak egy megépített rendszer tervezése, üzemeltetése, valamint hiba meghatározása során. Egy optikai hálózatban mindig van egy adó berendezés, amely legalább egy csatlakozó segítségével csatlakozik a fénytovábbító közegre, esetünkben az optikai szálra, majd ismételten egy csatlakozón keresztül egy vevő egységre, amely veszi az adó által kibocsájtott fényimpulzusokat, 75. számú ábra.



75. ábra. Egyszerű optikai kapcsolat modell Forrás:Saját rajz

Egyetlen szálkapcsolat kiépítéséhez, ez a minimális felépítés. A fénykapcsolat csak abban az esetben jön létre, ha az adó és vevő megfelelő vonali csillapítás mellett képes a fényjeleket átvinni. A fényvezető szál egyik legfontosabb paramétere a csillapítás, mivel ezen érték határozza meg azt a maximális távolságot, ami adó és vevő között létrejöhet jelismétlő regenerátor nélkül. A fény energiaveszteséget szenved, amíg az adótól a vevőig ér el. A csillapítás mértékét az adó oldalon beadott teljesítmény és „l" optikai átviteli út végén, a vevő oldali kilépő teljesítmény hányadosaként, majd a 10-es alapú logaritmusa tízszereseként számoljuk a 6. számú képlet alapján.

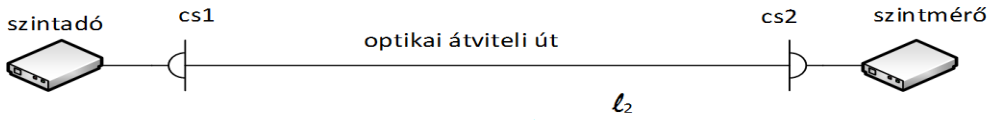
$$\alpha = 10lg\frac{P_{be}}{P_{ki}} \qquad [\text{dB}] \qquad (6)$$

Mivel a fényvezető hálózat elosztott paraméterű hálózat, az összefüggést megadhatjuk kilométerre vonatkozóan is az 7. képlet alapján. [187] [188] [189] [190]

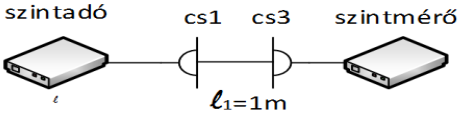
$$\alpha = \frac{10}{l} lg\frac{P_{be}}{P_{ki}} \quad [\frac{dB}{km}] \qquad (7)$$

Visszavágásos módszer

A visszavágásos módszer esetén, először az optikai szálvégen szintmérővel kell mérést végeznünk a 76. ábrának megfelelő összeállításban. Meg kell mérni a szintadóból érkező fényteljesítmény nagyságát. Ezután, közel kell mennünk az adóhoz, és ott körülbelül 1 méterre elvágva a fényvezető szálat, a 77. ábrának megfelelően csatlakozót szerelve a szálvégre, újabb mérést kell végeznünk, megmérve az adóból érkező jel teljesítményt. [191]



76. ábra Szálcsillapítás mérés visszavágásos módszer Forrás:Saját rajz



77. ábra Szálcsillapítás mérés visszavágott szál esetén Forrás:Saját rajz

A mérések eredményéből az alábbi 8. számú képlet segítségével meghatározhatjuk a kilométerenkénti csillapítást.

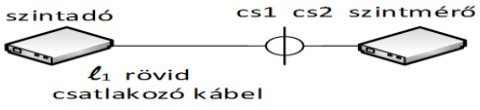
$$\alpha = \frac{1}{l_2 - l_1} * 10 \log \frac{P_{cs3}}{P_{cs2}} \quad [\frac{dB}{km}] \qquad (8)$$

Beiktatásos módszer

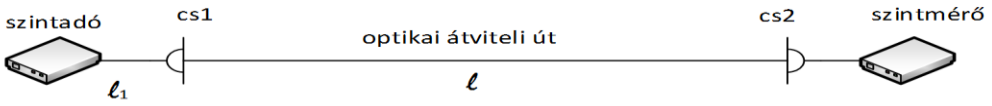
A beiktatásos módszer nagyban hasonlít a visszavágásos módszer elméletéhez, azonban itt elsőként egy rövid szálon a szintadó után mérjük meg a szintadó teljesítményét a 78. ábra szerint, majd ezután a megmérni kívánt szálvégen újból szintmérést végzünk. Ezt látható az 79. számú ábrán. [192] [193] [194] [195]

A szálcsillapítást a 9. számú képlettel számíthatjuk ki.

$$\alpha = \frac{1}{l - l_1} * 10 \log \frac{P_{cs1}}{P_{cs2}} \quad [\frac{dB}{km}] \qquad (9)$$



78. ábra Beiktatásos módszer első mérési összeállítás Forrás:Saját rajz

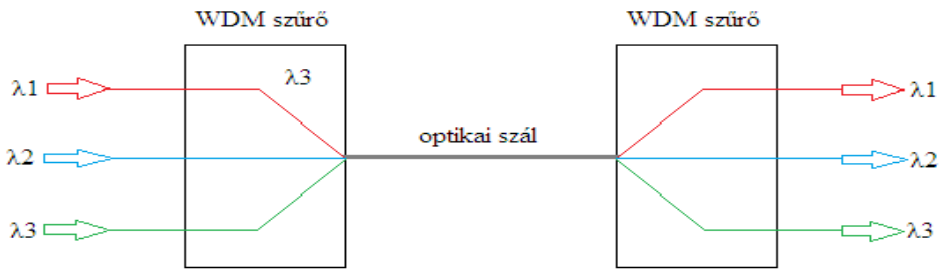


79. ábra Beiktatásos módszer második mérési összeállítás Forrás:Saját rajz

A két mérést összehasonlítva, az utóbbi megfelelőbbnek bizonyul akár egy üzemi mérés során is, mivel ebben az esetben nem kell elvágni a mérni kívánt szálat. Az optikai kábelhálózatok építése során, minden esetben készülnie kell csillapítás mérési jegyzőkönyvnek a későbbi visszaellenőrzés miatt. Hiba esetén, ez az első paraméter, amit meg kell vizsgálni. Előnye a mérés egyszerűsége, hátránya, hogy a szál mindkét végén beavatkozást igényel. A gyakorlatban a szintadót és szintvevőt célszerű a mérés elején egy rövid mérőkábel segítségével összekötni, és a referenciaszinteket egymáshoz képest beállítani. [196] [197] [198] [199] [200]

Optikai szálak OTDR-el (optical time-domain reflectometer) történő monitorozása

Az optikai távközlés eszközeinek fejlődésével létrejöttek a nagyon keskeny hullámhosszal rendelkező fényforrások. Ezek jellemzően nagy stabilitással képesek ugyan azt a keskeny hullámhosszat sugározni a kis kromatikus diszperzió megvalósítása céljából. Később a technológia fejlődésével megvalósulhatott, hogy megfelelő hullámhosszú szűrők alkalmazása mellett egy optikai szálon több adatátviteli csatorna is létrehozható lett, ezzel a sávszélességet jelentősen megnövelve. Ezt nevezik WDM (Wavelenght Division Multiplex) technológiának. Ezen belül van CWDM (Coarse Wavelenght Division Multiplex) és DWDM (Dense Wavelenght Division Multiplex) megoldások, amelyek elvüket tekintve megegyeznek, csak a távközlésre használt hullámhosszaik közötti távolság különbözik. A CWDM technológia esetén a csatornák távolabb vannak egymástól, mint a DWDM esetén. A technológia hullámhosszainak elkülönítésére használt szűrőket WDM szűrüknek nevezik. Az alábbi 80. számú ábrán három hullámhossz tekintetében látható szemléletes példa, az egy optikai szálon történő több hullámhossz átvitelére. [201] [148] [202]

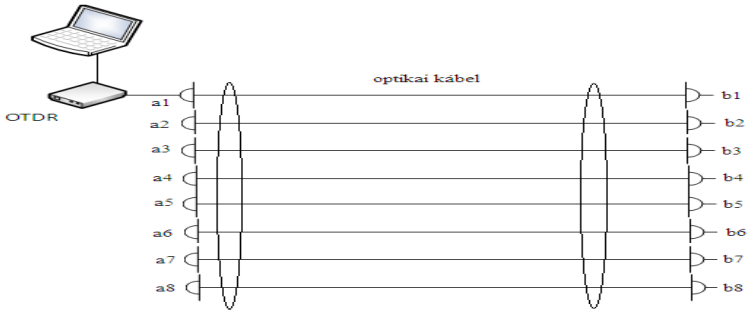


80. ábra Három sávos WDM szűrő Forrás:Saját rajz

Sötétszál felügyelet

A sötét szálfelügyelet esetén, egy optikai kábel egyik, a távközlésben nem résztvevő pót, vagy nem használt elemi fényvezető szálat mérünk OTDR műszerrel. Ez a mérés, nagyon jó tájékoztatást ad a kábel folytonosságáról, a feltételezett öregedési és csillapítási folyamatok változásáról. Nincs szükség drága szűrő és csatoló egységekre, azonban hátrányként megemlítendő, hogy nem ad valós képet arról az adatátvitelben résztvevő fényvezető állapotáról, amely releváns lehet. Persze ez a megoldás nem rossz, mivel egy kábelben a futó fényvezető szálak paraméterei megegyeznek, és egy kábelen belül egy szál figyelése körülbelül 98% biztonságot nyújt az üzem folytonosságának ellenőrzése során. Egy kábelben két szál figyelése 99% biztonságú ellenőrzést jelent, három szál figyelése pedig 99,8% biztonságot jelent. A megvalósítás során, mérlegelni kell a ráfordítás és az elérni kívánt biztonság költségét.

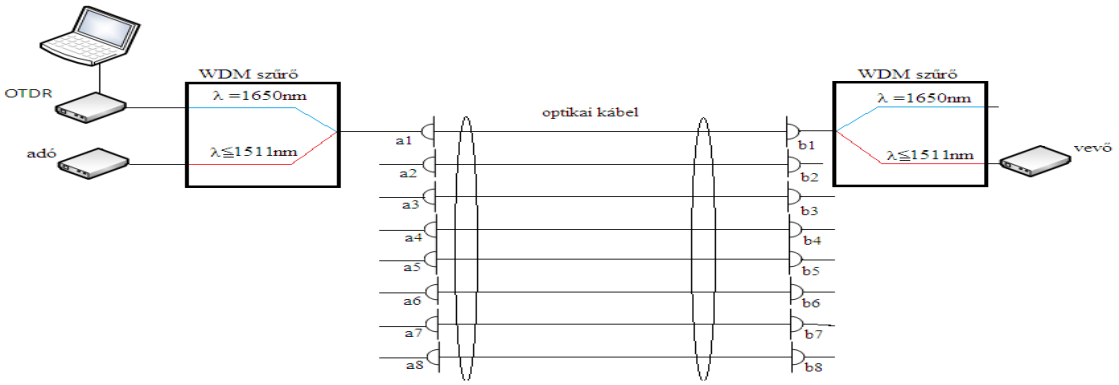
A sötétszál felügyelet jellemző mérőjel hullámhossza megegyezik a fénytávközlés szokásos 1310nm-es és 1550nm-es hullámhosszával. Az 1550nm alkalmazásával, a lehető legnagyobb mérési távolság érhető el, mert ezen a hullámhosszon a legkisebb a fényvezető szálak csillapítása. Kiépítése egy, a már meglévő kábelhálózat esetén is megvalósítható, amennyiben rendelkezik a hálózat szabad fényvezető szállal. A technológia egyszerű sematikus képe a 81. ábrán látható.



81. ábra ábra Sötétszál felügyelet egyszerűsített ábrája Forrás:Saját rajz

Sávon kívüli mérés „Out of Band”

A sávon kívüli mérés azon az elven alapul, hogy az optikai vezető szálban a legutolsó CDWM 1611nm-es hullámhosszú csatorna felett, 1650nm tartományba juttatunk mérő jeleket, majd azok visszaszóródásból eredő értéket jelenítjük meg az OTDR kijelzőjén 82. ábra. A hullámhosszra jellemző, hogy a törésekből és hajlításokból eredő csillapításokra érzékenyebb. A megvalósításához szűrő (WDM), egységekre is szükség van, tehát drágább, mint az előző megoldás. Hátrányként kell megemlíteni, hogy ha több elágazás van egy optikai szálban, akkor a pontos elágazások és az utánuk következő elemek csatlakozásából eredő visszaszórások egymástól nem különíthetőek el jól. Implementációját érdemes a kábelhálózat üzembeállítása előtt elvégezni. Természetesen ez a módszer a védett helyiségek esetén alkalmazott távközlésben résztvevő optikai szál 100%-os felügyeletét megvalósíthatja. [203]



82. ábra Sávon kívüli OTDR mérés egyszerűsített vázlata Forrás: Saját rajz

Sávon belüli mérés „In Band”

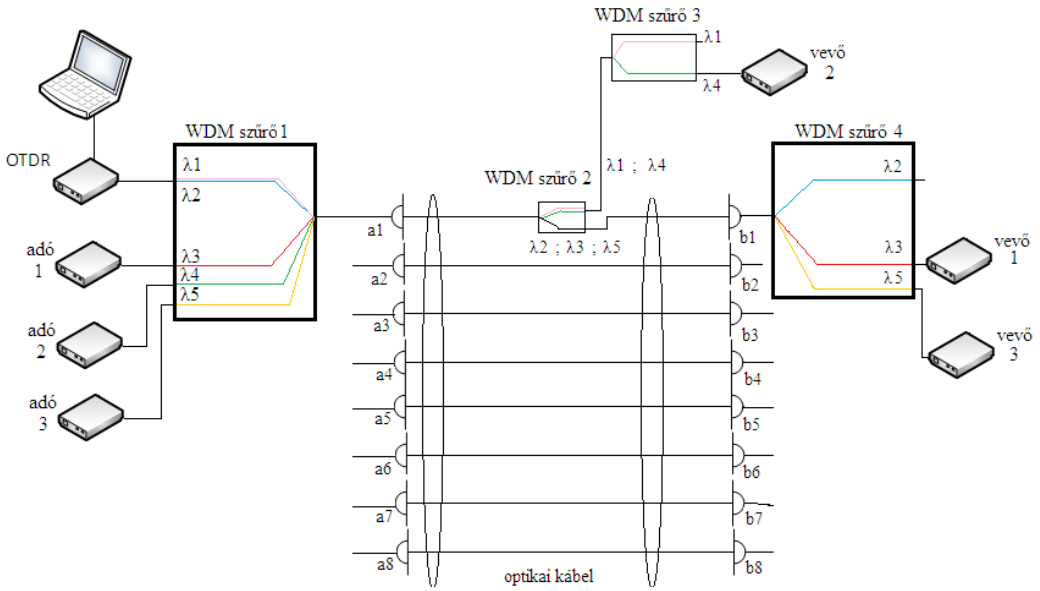
A módszer megvalósítása, hasonló a sávon kívüli módszeréhez, azonban ez az eljárás az adattovábbítás hullámhosszai közül használ egyet, vagy többet, a kialakítástól függően. A 83. ábrán egy elágazásos optikai szál monitorozhatóságának elvi sémáját láthatjuk. Az ábrán látható, hogy 5 darab, különböző λ hullámhossz van egy „WDM szűrő 1” segítségével a kábelre illesztve. A különböző hullámhosszak a szemléletesség kedvéért különböző színekkel vannak jelölve: λ1 rózsaszín, λ2 kék, λ3 piros, λ4 zöld, λ5 narancssárga. A λ1 és λ2 az OTDR hullámhosszai, míg λ3, λ4, λ5 az adattovábbítás

hullámhosszai. Amennyiben a fényvezetőben elágazás van, amely jelen ábrán „WDM szűrő 2 ”elnevezéssel van ellátva, a hullámhosszak megfelelő megválasztásával és megfelelő WDM szűrő alkalmazásával az elágazások elkülöníthetőek. Az ábrát szemlélve a „WDM szűrő 2 ” felső szárát követve λ1 és λ4 jut tovább, ebből λ1 az OTDR vizsgáló jele, λ4 az adatot hordozó jel, az alsó szárát követve, λ2, λ3, λ5 jutnak tovább, ebből λ2 az OTDR vizsgáló jele, λ3 és λ5 az adatot hordozó jelek.

A „WDM szűrő 3 „és „WDM szűrő 4 ” nevű szűrők, a végkészülékek számára választják szét a megfelelő hullámhosszat, hogy az adattovábbításra és monitorozásra használt jelek ne zavarják egymást.

Az OTDR műszer λ1 és λ2 hullámhosszai között váltva, az adott szakasz paramétereit vizsgálhatjuk. A λ1 OTDR vizsgálójel esetén a „WDM szűrő 1 ” – „WDM szűrő 2 ” – „WDM szűrő 3 ” vonalat. A λ2 OTDR vizsgálójel választása esetén a „WDM szűrő 1 ” – „WDM szűrő 2 ” – „WDM szűrő 4 ” vonalat.

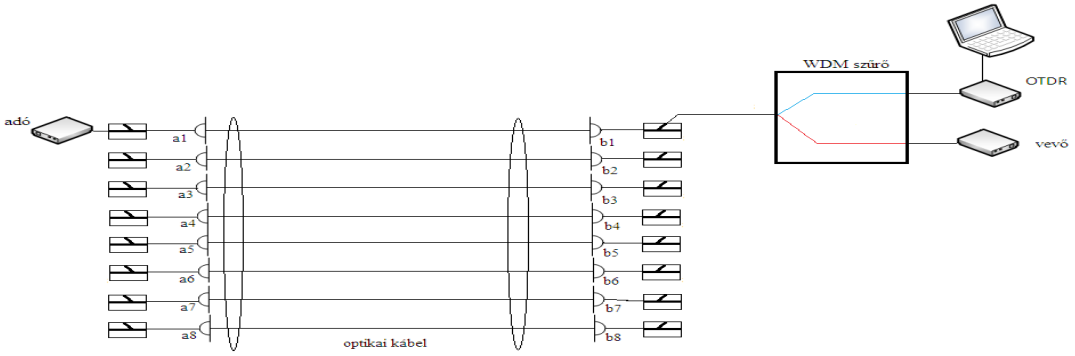
Ezen a példán keresztül láthatjuk, hogy egy optikai szálon több különböző hullámhosszú jel is továbbítható. Hátrányként megemlítendő, hogy a mérésre használt hullámhosszak adattovábbítása nem használhatóak, azonban ezen módon, útelágazásos szálfelügyelet is megvalósítható az OTDR kimenő hullámhosszainak változtatásával. A mérőrendszer már kiépített WDM szűrőkkel ellátott hálózatok esetén is beiktatható. Tekintettel kell lenni az adattovábbítás hullámhosszaira, keskeny sávszélességű optikai jel használatára van szükség. [203]



83. ábra Sávon belüli OTDR mérés egyszerűsített sematikus ábrája Forrás:Saját rajz

Szélessávú leágazó csatolókon keresztüli mérés

Az optikai hálózatok végpontjainál használatosak a teljes hullámtartományt átengedő szélessávú elágazások, amelyek segítségével a portok forgalma monitorozható 84. ábra. Ezen eszközön való mérőjel beadás és fogadás, OTDR mérés megvalósítására ad lehetőséget. Az itt beadott mérőjelet szintén elválasztó (WDM) szűrő segítségével adjuk be és fogadjuk, figyelembe véve, hogy a mérőjel hullámhossza ne essen egybe az adattovábbításra használt jel hullámhosszával. A megvalósítás szempontjából, a beadott jelet az adattovábbítás vételi oldalán táplálják be az interferenciák elkerülése végett.



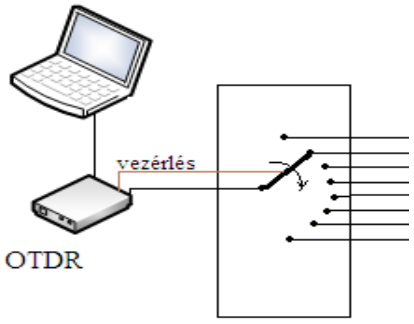
84. ábra OTDR műszer elágazásba való iktatásának sematikus képe Forrás: Saját rajz

Optikai kapcsoló használata a szálfelügyeletek kibővítésére

A példákban az OTDR-el történő szálfelügyeletet egy szálon vizsgáljuk. Azonban teljes ellenőrzés megvalósítása esetén, minden egyes szál mellé egy-egy OTDR műszer kellene. Ezt a költséges megoldást célzott kiváltani a szálkapcsoló berendezés megvalósítása, amely nélkül a korszerű szálfelügyeleti megoldások elképzelhetetlenek lennének.

A multiplexer elven működő egység Optical Test Access Unit (OTAU) nem más, mint az OTDR által vezérelt szálkapcsoló berendezés, amellyel a mérni kívánt szálba becsatoljuk a mérőjelet szolgáltató műszert. Megfelelő szoftveres vezérlés segítségével, továbbkapcsolva a szálakat, a méréseket folyamatosan ismételve folyamatos felügyeletet kapunk. A 85. ábra szemlélteti az optikai kapcsoló működését. A beadni kívánt OTDR jelek a csatornákhoz beállíthatóak, valamint a telepítés során referencia érték felvehető a mért értékek és diagramok tekintetében. Amennyiben a szál mérése

során a berendezés a referenciához képest hibát érzékel, azonnal riasztást generál. Ebben az esetben a kapcsolgatás gyakoriságától függ, hogy egy-egy szál mikor kerül sorra. Az újból sorra kerülés idejéből megkapjuk azt a legrövidebb időt, amire egy esetleges hibát érzékelni lehet. [204]



85. ábra Optikai kapcsoló sematikus ábrája Forrás:Saját rajz

A további fejlesztések a hibakimutatás gyorsaságának növelése irányába mutatnak, ezáltal az ellenőrzés alá vont optikai szálak vételi oldalán folyamatos teljesítménymérés valósul meg. A beüzemelés során a teljesítményszintek referenciaként vannak felvéve. A teljesítménymérő össze van kötve az OTDR-t vezérlő számítógéppel, így teljes felügyeleti egységet alkotva. Ha a folyamatos teljesítménymérő a referenciából való kicsúszást érzékeli, az OTDR-t azonnal a szál vizsgálatára irányítja. Így kiküszöbölhető az az időrés, amely kedvezőtlen átkapcsolási sorrend esetén állna fenn. [150] [205] [206] [207] [208]

Az optikai hálózatokon előforduló hibák és jellemzőik

Az optikai hálózatok hibáinak felsorolását számtalan megközelítéssel osztályozhatjuk. Esetünkben a legfontosabb hibafajta a vonali csillapítás megnövekedése. Az adóegység által kisugárzott maximális teljesítmény, a csillapítás növekedésének hatására nem jut el megfelelő szinten a vevő egységbe. A csillapítás negatív irányú változása az alábbiak miatt lehetséges:

- száljellemzők megváltozása;
- csatlakozók minőségének romlása;
- adóegység teljesítmény és vevőegység érzékenységének megváltozása.

Száljellemzők megváltozása

Az optikai szálak csillapítása főként a rájuk ható fizikai hatások miatt változhat meg.

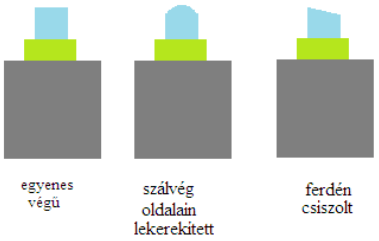
A kábelekben haladó szálak tekintetében, a kábelt érő csavaró, nyíró erők hatására, anyagszerkezeti feszültségek keletkeznek. Ezek a feszültségek a szálakban inhomogén helyeket hoznak létre, amelyeknek hatására lokális csillapítási helyek jönnek létre.

További jellemző hiba, a kábelek és ezzel együtt a szálak nagy szálirányú húzóerőnek való kitétele. Ez a behatás szintén anyagszerkezeti problémához vezet. Amennyiben egy optikai kábel, valamint a benne lévő szálak hosszirányú behatástól kárt szenvednek, lehetséges, hogy a teljes szakasz használhatatlanná válik. [209]

Építkezések folyamán előfordulhat a szálak keresztirányú törése, például munkagép általi átvágás esetén. Természetesen ez teljes szakadáshoz vezet, ami szálhegesztéssel, szakaszcserével javítható. Nem megfelelő kábelvezetésből is eredhet csillapítás növekedés, mégpedig a legkisebb hajlítási sugár alá való töréssel. Ebben az esetben, ha a szálak nem szenvednek maradandó károsodást, a hiba megszüntetésével a csillapítás visszaáll az eredeti paraméternek megfelelő állapotba. Ezeket a hibákat „makrobanding” makrohajlítási hibának hívják.

Csatlakozók minőségének romlása

Minden optikai rendszer csatlakozók segítségével kapcsolódik a hálózati elemekhez. A csatlakozók kábeltípusonként változnak. Jellemzően a csatlakozók hibáját mechanikus és szennyeződés okozta hibára vezethetjük vissza. A csatlakozókban a szálvégek lehetnek egyenes (flat) végződésűek, a szálvég oldalain lekerekített (PC , UPC) végződésű, valamint ferdén (8^o-os szögben) csiszolt (APC) típusúak 86. ábra.



86. ábra Csatlakozó típusok Forrás:Saját rajz

A csatlakozók egymáshoz illesztése, nagymértékben meghatározza a csillapítás értékét. Ha központossági hiba, vagy nagy légrés alakul ki, törésmutató változás lép fel a két fényvezető mag között, és így az átviteli útban nem kívánt csillapítást okoz.
Továbbá a csatlakozók szennyeződésmentes illesztését is biztosítani kell, mert ha szennyező anyag kerül a csatlakozó felületek közé, ott csillapítási hiba merül fel. [148] [202]

Adóegység teljesítmény és vevőegység érzékenységének megváltozása

Ebben az esetben valamilyen készülékhibára kell gondolnunk, amely nem függ az optikai hálózat csillapításától. Ez a hibafajta a végberendezések elromlását jelenti, aminek a megoldása az egységek cseréjével vagy az egységek javíttatásával oldható meg. [210] [211]

Az optikai szálfelügyeleti rendszerrel kimutatható egyéb hibák

Az optikai szálfelügyelettel az előzőekben felsorolt hibákon kívül, a lassú vagy időszakos csillapítási hibák is kimutathatóak. Ez azt jelenti, hogy a felügyeleti rendszer telepítésekor felvett teljes vonalszakaszt referencia értéknek tekintve, riasztási küszöböt állítunk be. Amikor az ellenőrzött szál csillapítása eléri a beállított érték szerinti alsó küszöbértéket, a felügyeleti központ értesítést generál.
A folyamatos szálfelügyelettel olyan hibák is kimutathatóak, amelyeket egyéb időszakos OTDR megoldással nehézkes kimutatni. Ha a hiba az idő nagy részében nem jelentkezik, és a szálparaméter nem tér el jelentősen a referencia értéktől csak pillanatokra, akkor a szálban valahol hirtelen megnövekszik a csillapítás.
Ilyen jellegű hiba lehet egy mechanikailag instabil csatlakozó, amely időközönként megmozdulva jelentősebb csillapítást eredményez, vagy az optikai szál időszakos megtörése, mint például egy rack szekrény valamely részéhez való nyomódása, becsípése.
A védett helyiségek kutatási témához kapcsolódva az optikai szálak információbiztonsági szempontból történő védelmének szintén alapvető eszköze a folyamatos szálfelügyeleti berendezés üzemeltetése. Az optikai szálak lehallgatásához csillapítási hiba társítható, amelyhez leágazás, vagy hajlítás szükséges. Az abból származó csillapítás is kimutatható lehet. Amennyiben a monitoring riasztási

küszöbértéke megfelelően érzékeny, úgy a kismértékű csillapítás megjelenése is jelezhetővé válik. [202]

KÖSZÖNETNYILVÁNÍTÁS

Jelen írás soraiban szeretnék köszönetet nyilvánítani a kutatás nehézségeinek leküzdésében részemre nyújtott segítségükért, a publikációkban való segítségnyújtásért, valamint az önzetlen emberi és szakmai segítségért az Óbudai Egyetem Biztonságtudományi Doktori Iskola, valamint a Kandó Kálmán Villamosmérnöki Kar Híradástechnikai Tanszék dolgozóinak. Külön köszönetet mondok **Dr. Varga Péter János docens úr** témavezetőmnek, és a Biztonságtudományi Doktori Iskola vezetőjének **Prof. Dr. Rajnai Zoltán egyetemi tanár úrnak** a támogató segítségükért, és a disszertáció megírásához vezető úton nyújtott támogatásukért. Köszönöm a Doktori Iskola adminisztrátor hölgyeinek, **Farkasné Hronyecz Erikának és Lévay Katalinnak**, hogy segítették és koordinálták tanulmányaimat.

Köszönetet mondok családtagjaimnak, **kisfiamnak Gábornak**, **páromnak Beátának** és a **Szüleimnek** az értekezés megírása alatt tanúsított türelmükért.

Továbbá szeretnék köszönetet mondani **kollégáimnak** a hatékony és célravezető együtt gondolkodásokért.

Budapest, 2022. október 25. Bréda Gábor