

Celkové náklady na životnost bezpečnostních technologií

Roman Kostelník

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Roman Kostelník
Osobní číslo: A21025
Studijní program: B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia: Prezenční
Téma práce: Celkové náklady na životnost bezpečnostních technologií
Téma práce anglicky: Total Cost of Ownership in Security Technologies

Zásady pro vypracování

- Vypracujte literární rešerši zabývající se problematikou Total Cost of Ownership (TCO) v bezpečnostních technologiích a systémech.
- Navrhněte experimenty pro testování TCO u vybraných zástupců VSS a PZTS.
- Stanovte faktory ovlivňující TCO u VSS a PZTS.
- Zhotovte matematický model zahrnující faktory TCO pro různé scénáře a evaluační algoritmus.
- Vyhodnoťte a analyzujte výsledky získané algoritmem.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. HEILALA, J.; HELIN, K. a MONTONEN, J. Total cost of ownership analysis for modular final assembly systems. Online. International Journal of Production Research. 2006, roč. 44, č. 18-19, s. 3967-3988. ISSN 0020-7543. Dostupné z: <https://doi.org/10.1080/00207540600806448>.
2. RODA, Irene; MACCHI, Marco a ALBANESE, Saverio. Building a Total Cost of Ownership model to support manufacturing asset lifecycle management. Online. Production Planning & Control. 2020, roč. 31, č. 1, s. 19-37. ISSN 0953-7287. Dostupné z: <https://doi.org/10.1080/09537287.2019.1625079>.
3. GULLO, Louis J. a DIXON, Jack. Design for maintainability. Hoboken, NJ: John Wiley & Sons, 2021. ISBN 9781119578536. Dostupné také z: <https://proxy.k.utb.cz/login?url=https://onlinelibrary.wiley.com/doi/book/10.1002/9781119578536>
4. ADÁMEK, Milan; BARČOVÁ, Karla; BITALA, Petr; MACH, Václav a ŠEVČÍK, Jiří. Dohledové videosystémy v bezpečnostních technologiích. SPBI Spektrum. Červená řada. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2022. ISBN 978-80-7385-263-4.
5. ČSN EN 50131-1 ed. 2 (334591) Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky. Praha: Český normalizační institut, 2007.

Vedoucí bakalářské práce: **Ing. Stanislav Kovář, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **11. prosince 2024**
Termín odevzdání bakalářské práce: **2. června 2025**



doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 11. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....

podpis autora

ABSTRAKT

Bakalárska práca sa zaoberá problematikou celkových nákladov na životnosť bezpečnostných technológií, konkrétne videosystémov a poplachových zabezpečovacích a tiesňových systémov. Cieľom práce je vypracovať literárnu rešerš, navrhnúť experimenty pre testovanie TCO, stanoviť faktory ovplyvňujúce TCO, zhotoviť matematický model TCO pre rôzne scenáre s evaluačným algoritmom a následne vyhodnotiť a analyzovať získané výsledky. Teoretická časť definuje TCO, jeho históriu, metodiky výpočtu a relevantné faktory a tiež popisuje VSS a PZTS. Praktická časť zahŕňa merania spotreby elektrickej energie a dátovej náročnosti vybraných IP kamier a PZTS ústredne. Na základe nameraných dát a odhadovaných cien je zostavený matematický model TCO. Tento model je aplikovaný na rôzne scenáre, pričom sú analyzované jednotlivé nákladové zložky. Výsledky poukazujú na dominantný vplyv nákladov na cloudové úložisko v celkovom TCO pre VSS, zatiaľ čo náklady na energiu sú relatívne nízke. Práca prináša praktický model a metodiku pre hodnotenie ekonomickej náročnosti bezpečnostných systémov.

Kľúčové slová: celkové náklady na vlastníctvo, TCO, bezpečnostné technológie, dohľadové video systémy, VSS, poplachové zabezpečovacie a tiesňové systémy, PZTS, matematický model, analýza nákladov

ABSTRACT

This bachelor thesis deals with the Total Cost of Ownership (TCO) of security technologies, specifically Video Surveillance Systems (VSS) and Intrusion and Hold-up Alarm Systems (IAS). The aim of this thesis is to conduct a literature review, design experiments for TCO testing, determine TCO influencing factors, create a mathematical TCO model for various scenarios with an evaluation algorithm, and subsequently evaluate and analyze the obtained results. The theoretical part defines TCO, its history, calculation methodologies, and relevant factors, and also describes VSS and IAS. The practical part includes measurements of electricity consumption and data storage requirements for selected IP cameras and an IAS control panel. Based on the measured data and estimated prices, a mathematical TCO model is developed. This model is applied to different scenarios, analyzing individual cost components. The results highlight the dominant impact of cloud storage costs on the overall

TCO for VSS, while energy costs are relatively low. The thesis provides a practical model and methodology for assessing the economic demands of security systems.

Keywords: Total Cost of Ownership, TCO, security technologies, Video Surveillance Systems, VSS, Intrusion and Hold-up Alarm Systems, IAS, mathematical model, cost analysis

Na tomto mieste by som sa chcel poďakovať všetkým, ktorí mi akýmkoľvek spôsobom pomohli pri písaní tejto bakalárskej práce.

Moje poďakovanie patrí predovšetkým môjmu vedúcemu bakalárskej práce, Ing. Stanislavovi Kováňovi, PhD., za jeho odborné vedenie, cenné rady, pripomienky a čas, ktorý mi venoval počas konzultácií.

V neposlednej rade ďakujem mojej rodine, priateľke a priateľom za ich trpezlivosť, podporu a povzbudenie počas celého štúdia a písania tejto práce.

OBSAH

ÚVOD.....	15
I TEORETICKÁ ČASŤ	18
1 DEFINÍCIA POJMU CELKOVÉ NÁKLADY NA ŽIVOTNOSŤ.....	19
1.1 HISTÓRIA TCO.....	19
1.2 NÁKLADY ŽIVOTNÉHO CYKLU A CELKOVÉ NÁKLADY NA ŽIVOTNOSŤ.....	20
1.2.1 Rozdiel medzi LCC a TCO	20
1.3 VÝHODY A NEVÝHODY TCO.....	21
1.4 VÝPOČET TCO	21
1.5 FAKTORY OVPLYVNÚJÚCE TCO	22
1.5.1 Úvahy o faktoroch TCO dnes	23
1.6 VÝZVY PRI VÝPOČTOCH TCO.....	24
2 DOHĽADOVÉ VIDEO SYSTÉMY	25
2.1 ZÁKLADNÉ ČASTI DOHĽADOVÝCH VIDEOSYSTÉMOV	25
2.2 ANALÓGOVÉ KAMERY	27
2.2.1 Princíp činnosti analógových kamier	27
2.2.2 Výhody analógových kamier	28
2.2.3 Nevýhody analógových kamier.....	29
2.3 IP KAMERY	30
2.3.1 Princíp činnosti IP kamier	31
2.3.2 Bežné konfigurácie a typy IP kamier	32
2.3.3 Výhody IP kamier	33
2.3.4 Nevýhody IP kamier	34
2.3.5 Odporúčania pri prechode na IP systém.....	35
2.4 OPTICKÉ PRVKY KAMIER	36
2.4.1 Obrazový senzor.....	37
2.4.2 Objektív.....	39
2.5 FAKTORY OVPLYVNÚJÚCE VSS.....	40
2.5.1 Vlastnosti moderného systému	42
2.5.2 Kľúčové faktory pri rozhodovaní.....	43
2.6 KONKRÉTNE KAMERY	43
2.6.1 AXIS M1045-LW	43
2.6.2 AXIS Q1635.....	45
2.6.3 AXIS P1435-LE	47
2.6.4 AXIS P3225-LVE Mk II.....	49
2.6.5 AXIS Q3505-V	50
3 POPLACHOVÉ ZABEZPEČOVACIE A TIESŇOVÉ SYSTÉMY	52
3.1 PRVKY PZTS.....	53

3.1.1	Prvky plášťovej ochrany.....	53
3.1.2	Prvky priestorovej ochrany	60
3.1.3	Prvky predmetovej ochrany.....	68
3.1.4	Prvky perimetrickej ochrany	70
II	PRAKTICKÁ ČASŤ	74
4	ÚVOD K MERANIAM.....	75
5	MODEL VÝPOČTU CELKOVÝCH NÁKLADOV NA VLASTNÍCTVO (TCO).....	76
5.1	ZARADENIE TCO NÁKLADOV PODĽA FÁZ ŽIVOTNÉHO CYKLU	78
5.2	ANALÝZA KATEGÓRIE NÁKLADOV.....	79
5.3	MATEMATICKÝ MODEL TCO A PRAKTICKÝ EVALUAČNÝ ALGORITMUS.....	85
5.3.1	Základné zložky modelu TCO:	85
5.3.2	Celkové náklady na vlastníctvo v tomto modeli:	86
5.3.3	Modelovanie TCO pre rôzne scenáre	86
5.3.4	Praktický evaluačný algoritmus	86
6	SCENÁRE A PODMIENKY TESTOVANIA	88
7	MERANIE SPOTREBY ELEKTRICKEJ ENERGIE	92
7.1	POSTUP MERANIA	92
7.2	SPRACOVANIE ÚDAJOV	93
8	MERANIE DÁTOVEJ NÁROČNOSTI VIDEOZÁZNAMU	95
8.1	CIEĽ MERANIA A METODIKA	95
8.2	ZISTENIA A PRIEBEŽNÉ HODNOTENIE	95
8.3	DÁTA GENEROVANÉ ZA DEŇ A MESIAC	96
9	VÝPOČET NÁKLADOV NA ENERGIU A ÚLOŽISKO.....	98
9.1	VÝPOČET NÁKLADOV NA ELEKTRICKÚ ENERGIU	98
9.2	VÝPOČET NÁROKOV NA ÚLOŽISKO	99
10	POROVNANIE ZARIADENÍ Z HĽADISKA NÁROČNOSTI.....	102
11	INTERPRETÁCIA VÝSLEDKOV A ODPORÚČANIA	104
11.1	VÝPOČET CELKOVÝCH ROČNÝCH NÁKLADOV.....	104
12	PREPOJENIE VÝSLEDKOV S TCO MODELOM.....	106
13	MERANIE SPOTREBY ELEKTRICKEJ ENERGIE ÚSTREDNE A PERIFÉRNÝCH ZARIADENÍ.....	108
14	ZHRNUTIE A INTERPRETÁCIA VÝSLEDKOV TCO PRE CELÝ SYSTÉM PZTS.....	111
14.1	REKAPITULÁCIA VÝSLEDKOV TCO PODĽA MODELOVÝCH SCENÁROV.....	111
14.2	ANALÝZA NÁKLADOVÝCH ZLOŽIEK TCO	112
14.3	POROVNANIE KOMPONENTOV A SCENÁROV.....	112
14.4	VPLYV KĽÚČOVÝCH PARAMETROV A CITLIVOSŤ MODELOV.....	113

14.5	OBMEDZENIA APLIKOVANÉHO MODELU	114
14.6	ZÁVERY A PRAKTICKÉ ODPORÚČANIA VYPLÝVAJÚCE Z ANALÝZY	114
ZÁVER		116
ZOZNAM POUŽITEJ LITERATÚRY		119
ZOZNAM OBRÁZKOV		123
ZOZNAM TABULIEK		124
ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK		125

ÚVOD

Bezpečnostné technológie, ako sú dohľadové video systémy (VSS) a poplachové zabezpečovacie a tiesňové systémy (PZTS), zohrávajú v súčasnosti kľúčovú úlohu pri ochrane osôb a majetku. Rozhodovanie o implementácii alebo modernizácii týchto systémov je často ovplyvnené nielen ich technickými parametrami a funkčnosťou, ale aj ekonomickými aspektami. Pri posudzovaní nákladov je však často braná do úvahy len počiatočná obstarávacía cena, čo môže viesť k neúplnému obrazu o skutočnej finančnej náročnosti danej technológie počas celej doby jej používania. Komplexnejší prístup ponúka metodika celkových nákladov na vlastníctvo (TCO), ktorá zahŕňa všetky priame aj nepriame náklady spojené s akvizíciou, prevádzkou, údržbou a likvidáciou systému.

Cieľom tejto bakalárskej práce je komplexne sa venovať problematike TCO v kontexte bezpečnostných technológií VSS a PZTS. Práca si kladie za úlohu splniť nasledujúce body:

1. vypracovať literárnu rešerš zameranú na problematiku TCO v bezpečnostných technológiách a systémoch;
2. navrhnúť experimenty pre testovanie TCO u vybraných komponentov VSS a PZTS;
3. stanoviť faktory ovplyvňujúce TCO u VSS a PZTS;
4. zhotoviť matematický model zahrňujúci faktory TCO pre rôzne scenáre a evaluačný algoritmus;
5. vyhodnotiť a analyzovať výsledky získané aplikáciou tohto algoritmu.

Práca je rozdelená na teoretickú a praktickú časť. Teoretická časť sa v prvej kapitole venuje definícií pojmu TCO, jeho historickému vývoju, metodike výpočtu, výhodám a nevýhodám, ako aj faktorom ovplyvňujúcim TCO. Následne sú v kapitolách 2 a 3 podrobne popísané dohľadové video systémy a poplachové zabezpečovacie a tiesňové systémy, vrátane ich základných komponentov a princípov činnosti.

Praktická časť nadväzuje na teoretické poznatky. Kapitola 4 uvádza do realizovaných meraní. Kapitola 5 predstavuje všeobecný model výpočtu TCO a analýzu nákladových kategórií, na čo nadväzuje podkapitola 5.3, ktorá definuje špecifický matematický model TCO a praktický evaluačný algoritmus vyvinutý v rámci tejto práce. V kapitole 6 sú opísané scenáre a podmienky testovania. Nasledujúce kapitoly 7 a 8 detailne popisujú metodiku a výsledky meraní spotreby elektrickej energie a dátovej náročnosti videozáznamu

vybraných VSS kamier. Na základe týchto meraní sú v kapitole 9 vypočítané náklady na energiu a úložisko. Kapitoly 10, 11 a 12 sa venujú porovnaniu zariadení, interpretácii výsledkov a prepojeniu s modelom TCO. Kapitola 13 obsahuje merania spotreby pre systém PZTS. Vyvrcholením praktickej časti je kapitola 14, ktorá sumarizuje a komplexne analyzuje výsledky TCO získané aplikáciou vyvinutého algoritmu na rôzne scenáre, pričom identifikuje kľúčové nákladové položky a rozoberá vplyv rôznych parametrov.

Prínosom práce je poskytnutie uceleného pohľadu na TCO bezpečnostných technológií a zhotovenie prakticky využiteľného modelu pre odhad a porovnanie nákladov, čo môže byť nápomocné pri rozhodovacích procesoch v oblasti investícií do bezpečnosti.

I TEORETICKÁ ČASŤ

1 DEFINÍCIA POJMU CELKOVÉ NÁKLADY NA ŽIVOTNOSŤ

Celkové náklady na životnosť (Total Cost of Ownership) ďalej už len ako TCO sú definované dvoma spôsobmi a to všeobecným a špecifickým pre oblasť informačných technológií. Vo všeobecnosti sú TCO chápané ako finančný odhad všetkých či už priamych alebo nepriamych nákladov, ktoré sú spojené s nakúpeným alebo nadobudnutým majetkom počas celej jeho životnosti, očakávanej dĺžky života alebo životného cyklu. Tento odhad je využívaný na to, aby sa spotrebiteľom a manažérom podnikateľských subjektov umožnilo určiť celkové náklady na vlastníctvo daného produktu, systému alebo iných aktív. [1]

V skratke možno uviesť, že pri posudzovaní TCO nemá byť zohľadnená iba obstarávacía cena. Do výpočtu majú byť zahrnuté aj všetky dlhodobé výdavky ako údržba, aktualizácie systému, školenie personálu ale aj prevádzkové náklady spojené s hardvérom a softvérom. Z toho vyplýva, že hoci môže byť systém na začiatku obstaraný lacnejšie, investícia sa z dlhodobého hľadiska nemusí vyplatiť. Pri rozhodovaní o nákupe majetku býva TCO sledované podnikmi aj jednotlivcami, keďže do analýzy sú započítané nielen priame náklady, ale aj všetky nepriame výdavky. Kým priame výdavky môžu byť zaznamenané pomerne jednoducho, nepriame náklady bývajú charakterizované väčšou rozmanitosťou a ich identifikácia je náročnejšia. Práve ich celková výška ovplyvňuje výslednú cenu. Finálna suma TCO je následne používaná ako rozhodujúce kritérium pri posudzovaní, či sa v projekte alebo investícii bude pokračovať. [2]

1.1 História TCO

Rôzne postupy na výpočet TCO sú zaznamenané už najmenej od 20. storočia. Dnešná, všeobecne prijímaná interpretácia TCO však vychádza z roku 1987, kedy poradenská spoločnosť Gartner Group formalizovala a propagovala tento koncept na hodnotenie nákladov infraštruktúry informačných technológií, ďalej už len ako IT. Avšak uvedené tvrdenie nemôže byť považované za úplne presné. Už v roku 1929, teda o 58 rokov skôr, boli v Manual of the American Railway Association definované komplexné finančné výpočty, v ktorých boli zohľadnené náklady vlastníctva prostredníctvom konceptu TCO. Týmto konceptom bola pri analýzach financovania pokrytá nielen fáza obstarania, ale aj celý životný cyklus sledovanej technológie. Následne bolo podrobnými štúdiami spoločnosti Gartner Group preukázané, že viac ako 80% celkových nákladov na informačné a komunikačné technológie vzniká až po nákupe zariadení, pričom s viac ako polovicou týchto výdavkov nie je v rozpočtoch vôbec počítané. [1]

1.2 Náklady životného cyklu a celkové náklady na životnosť

Celkové náklady životného cyklu (Life cycle costs) ďalej už len ako LCC sú definované ako súčty odhadovaných výdavkov, ktoré sú od okamihu vzniku myšlienky až po likvidáciu zariadenia alebo projektu určené analytickým štúdiom a odhadom všetkých nákladov vzniknutých počas ich životnosti. Analýzou LCC má byť vybrané riešenie spomedzi alternatív, pri ktorom bude dosiahnutá najnižšia dlhodobá cena vlastníctva. Do úvahy majú byť pritom zahrnuté položky spojené s návrhom, vývojom, výrobou, prevádzkou, údržbou, podporou a konečným vyradením významného systému v priebehu predpokladanej doby jeho využívania. Metodika LCC býva bežne uplatňovaná v procesnom priemysle, rovnako ako pri energetických technológiách či stavebných projektoch. Pre oblasť IT sa používa koncept TCO. [3]

1.2.1 Rozdiel medzi LCC a TCO

LCC je považované za širší prístup, zatiaľ čo TCO je definované ako užšie zameraná analýza nákladov, ktorej hranica sa začína vlastníctvom aktíva.

Tabuľka 1 Rozdiel medzi LCC a TCO

Oblasť porovnania	LCC	TCO
Časový rozsah	Sú zohľadňované náklady od úplného začiatku konceptu / návrhu cez vývoj, výrobu, obstaranie, prevádzku, údržbu až po likvidáciu aktíva	Sú počítané náklady od okamihu, keď sa aktívum dostane do vlastníctva používateľa až po jeho vyradenie.
Zahrnuté fázy	Do prepočtu sú vkladané pred investičné výdavky, investičné výdavky a všetky prevádzkové výdavky vrátane likvidácie	Sú zahrnuté investičné a prevádzkové výdavky plus náklady na ukončenie životnosti. Fázy pred nákupom zvyčajne zahrnuté nebývajú
Uhol pohľadu	Je uplatňovaný celkový systémový pohľad. Hodnotí sa, ktorú z alternatív sa oplatí realizovať z hľadiska celého hospodárskeho cyklu	Je aplikovaný pohľad vlastníka alebo prevádzkovateľa. Sleduje sa, koľko bude stáť vlastníctvo a prevádzka už vybranej technológie.
Typické využitie	Býva používané pri strategickom plánovaní, navrhovaní infraštruktúr, energetických technológií a stavebných projektov	Býva využívané pri taktických a operačných rozhodnutiach
Rozsah nákladových položiek	Okrem nákladov užívateľa môžu byť započítavané aj externé vplyvy	Do výpočtu sú zahrnuté priame a nepriame náklady vlastníka, prípadne rizikové položky
Praktický dôsledok pre bezpečnostné technológie	Pri navrhovaní rozsiahlych monitorovacích alebo poplachových systémov môže byť LCC použitá na optimalizáciu už v štádiu návrhu	Pri obstarávaní konkrétneho kamerového systému alebo poplachových zabezpečovacích a tiesňových systémov sa TCO používa na porovnanie dodávateľov

(upravené z: [4])

1.3 Výhody a nevýhody TCO

Za hlavnú výhodu TCO býva považovaná schopnosť odhaliť budúce výdavky, ktoré nebývajú zrejmé pri prvotnom nákupe položky. Keďže sa však metrika orientuje výlučne na náklady, pri jej bezvýhradnom uplatnení nasleduje stratégia, v ktorej sú minimalizované výdavky namiesto maximalizácie celkových prínosov. Ročná hodnota TCO je považovaná za vhodný indikátor priebežných nákladov a býva používaná ako prognóza pri tvorbe rozpočtu. Keď je TCO spriemerované za celé sledované obdobie, býva získavaná rozumná metrika na porovnanie podobných riešení. Priemerná hodnota však neposkytuje informáciu o časovom rozložení nákladov. Produkt s nízkou obstarávacou cenou a vysokými nákladmi na údržbu býva posudzovaný ako menej atraktívny než produkt s vyššou vstupnou cenou a nižšími priebežnými výdavkami, hoci môže byť dosahované rovnaké TCO počas analyzovaného obdobia. Za hlavný nedostatok pri TCO býva považované, že pri samostatnom použití je poskytovaný len veľmi úzky pohľad na náklady, pričom prínosy sú úplne ignorované. Za cieľ má byť pokladaný nie výber najlacnejšej aplikácie, ale obstaranie takej, ktorá prinesie podniku najvyššiu návratnosť. Ani určovanie priorít projektov nebýva metrikou TCO podporované. Ak by boli projekty radené len podľa najnižších nákladov, nebolo by do nich nikdy investované. Namiesto toho má byť realizované zvažovanie nákladov, prínosov a rizika portfólia, aby bolo rozhodnuté, ktoré projekty budú uprednostnené. Finančná disciplína je síce považovaná za dôležitú a v každej spoločnosti má byť zabezpečené jasné pochopenie priebežných nákladov spojovaných s technologickými investíciami. Na metrike TCO býva sústredovaná pozornosť najmä preto, že je poskytované hmatateľné číslo, na základe ktorého môže byť prijaté rozhodnutie o nižších výdavkoch. Keďže však technológie môžu výrazne ovplyvniť hospodársky výsledok, za vhodnejšie býva považované zohľadnenie celkového obrazu nákladov a prínosov, aby bola obstaraná nie najlacnejšia, ale najvhodnejšia alternatíva pre organizáciu. [5]

1.4 Výpočet TCO

Pred samotným stanovením celkových nákladov vlastníctva je najskôr nutné uplatniť ucelený postup, ktorým sa zabezpečí systematické zachytenie, vyčíslenie a priebežná kontrola všetkých relevantných výdavkov počas celého životného cyklu technológie. Na tento účel sa v praxi osvedčil nasledujúci päťkrokový rámec:

- **zhromaždenie údajov o všetkých nákladových faktoroch** - do prehľadu má byť zahrnutá nákupná cena, školenie zamestnancov, údržba, opravy a ďalšie výdavky, aby boli všetky náklady zachytené s presnosťou;
- **odhadnutý celkový náklad každej položky za celý životný cyklus produktu** - pri výpočte má byť zohľadnená životnosť, intenzita využívania a možné dodatočné výdavky, čím je zabezpečené realistické posúdenie budúcich nákladov;
- **sčítanie odhadov** - súhrnnou kalkuláciou celkových nákladov je poskytovaný jasný prehľad, čím sa uľahčuje kvalifikované rozhodovanie;
- **analýza TCO pravidelne revidovaná a aktualizovaná** - zmeny v cenách alebo spôsobe využívania majú byť priebežne zapracovávané, aby bola zachovaná presnosť výpočtov a aby bolo možné identifikovať príležitosti na optimalizáciu nákladov;
- **identifikácia dodatočných prínosov a stimulácie znižujúce celkové náklady** - do úvahy majú byť brané daňové úľavy, množstevné zľavy alebo nový softvér zvyšujúci efektívnosť, vďaka čomu sa môže výsledná nákladová bilancia ďalej zlepšiť. [6]

1.5 Faktory ovplyvňujúce TCO

Na TCO pôsobí mnoho faktorov a ich význam býva odlišovaný podľa fázy životného cyklu daného objektu:

- **v dodávateľskej kategórii** – životný cyklus začína návrhom produktu, po ktorom býva riadený produkt a následne sú obstarávané materiály. Po doručení materiálov býva spúšťaná výroba;
- **v kategórii služieb** – býva proces ktorý sa otvára iniciačnou fázou projektu. Po nej býva vykonávané hodnotenie a prechodové kroky, následne býva prevádzka služby udržiavaná a napokon býva realizované ukončenie;
- **zo strany spotrebiteľa** – životná fáza produktu býva zahájená jeho výberom, následne je sprevádzaná nákupom a používaním, až je nakoniec ukončená po skončení jeho životnosti.

Každá z týchto kategórií býva charakterizovaná rozdielnymi komponentmi TCO. Pri praktickom výpočte má byť zohľadnená každá etapa a proces, ktoré generujú náklady,

lebo niektoré položky môžu významne ovplyvniť iba jednu kategóriu, zatiaľ čo v iných prípadoch býva ich vplyv na celkovú cenu minimálny. Na základe štúdia literatúry bývajú všetky faktory TCO zhromažďované a zosumarizované, aby mohli byť zoskupené do troch hlavných zložiek:

- **jednorazové náklady** – bývajú započítavané náklady vzniknuté iba raz, ako obstarávacia cena, dotácie alebo dane, infraštruktúra, hodnota pri vyradení či ďalší predaj a registračné poplatky;
- **opakované (priebežné) náklady** – bývajú zahrnuté výdavky, ktoré vznikajú počas celej životnosti produktu, napríklad energia, údržba a servis, poistenie či dane. Obstarávacia cena sa často rozdeľuje na podfaktory výberu, výrobných nákladov, marže, dopravy a školenia;
- **sociálne náklady** – v niektorých prístupoch bývajú pripočítavané výdavky, ktoré znáša spoločnosť, ako emisie, hluk, nehody, dopravné zápchy alebo klimatické zmeny, zatiaľ čo v iných štúdiách bývajú zo samotnej kalkulácie TCO vynechávané.

Vo všeobecnosti bývajú všetky environmentálne emisie prepočítavané na peňažnú hodnotu, aby mohla byť dosiahnutá úplná projekcia finančnej záťaže spájanej s vlastníctvom. [7]

1.5.1 Úvahy o faktoroch TCO dnes

Okrem vyššie uvedených faktorov, môže TCO zahrňovať v modernej dobe aj tieto položky:

1. náklady na cloud computing a softvér ako službu (Software as a Service) ďalej už len ako SaaS;
 - modelmi predplatného SaaS bývajú zavádzané nepredvídateľné dlhodobé výdavky;
 - na TCO bývajú pôsobené skryté poplatky za ukladanie dát, volania aplikačných rozhraní a závislosť od jedného dodávateľa;
 - poplatky za odsun dát z cloudu, teda za presun údajov mimo poskytovateľa, bývajú často prehliadané.
2. optimalizácia nákladov podporovaná umelou inteligenciou (Artificial Intelligence) ďalej už len ako AI;

- náklady na údržbu sú predikované umelou inteligenciou a výdavky na IT infraštruktúru sú na jej základe optimalizované;
- budúce zmeny cien u dodávateľov sú odhadované pomocou prediktívnej analytiky.

3. udržiateľnosť a zelené IT;

- do výpočtu TCO sú započítavané energeticky úsporné servery, cloudové dátové centrá aj dosiahnuté zníženie uhlíkovej stopy;
- náklady na súlad sú navyšované o požiadavky regulácií, ktoré sa týkajú správy a vykazovania udržiateľnosti. [8]

1.6 Výzvy pri výpočtoch TCO

Viacere metodiky a softvérové nástroje sú používané na výpočet TCO, no postup žiaden postup nie je považovaný za bezchybný. V mnohých podnikoch nebýva vytvorená jednotná metodika, v dôsledku čoho nie sú nákupné rozhodnutia prijímané na základe jednotných údajov. Určenie rozsahu prevádzkových nákladov pre jediný kus IT vybavenia sa vyznačuje náročnosťou. Skryté faktory, ako dopisy či záruka, bývajú ľahko prehliadané alebo sa porovnávajú nepresne. Napríklad podpora jedného servera je často oceňovaná vrátane ceny náhradných dielov, tým je podpora zdražovaná, ale je eliminovaný obstarávací náklad na nový systém. V analýzach nákladov vlastníctva nebýva predvídané neočakávané zvyšovanie cien v čase čo znamená že ak sú ceny dielov prudko navýšené v dôsledku zmeny distribútora, nie je táto skutočnosť zachytená. Do výpočtu TCO nemôže byť zapracovaná disponibilita budúcich modernizácií či služieb ani vplyv dodávateľských vzťahov. [8]

2 DOHLADOVÉ VIDEO SYSTÉMY

Kamerové systémy sú už viac než päťdesiat rokov považované za neoddeliteľnú súčasť bezpečnostného priemyslu. Bez ohľadu na to, či boli označované ako Priemyselná TeleVízia, ďalej už len ako PTV, alebo neskôr ako uzavretý televízny okruh (Closed Circuit TeleVision) ďalej už len ako CCTV, vždy boli koncipované na princípe uzavretých televíznych okruhov. Systémy PTV alebo CCTV boli využívané na monitorovanie záujmových oblastí a ich charakteristickou črtou bola uzavretosť, takže k nim nebolo možné pristupovať na diaľku. Kamerový systém (Video Surveillance System), ďalej už len ako VSS je dnes chápaný ako zostava kamerového vybavenia, úložiska, doplnkových zariadení určených na prenos obrazu a diaľkového ovládania. V nových štandardoch, ktoré sú používané pri návrhu kamerových systémov na báze technológií internetového protokolu, ďalej už len ako IP, je pozorovaný odklon od predtým zaužívanej skladby takýchto systémov. Napriek týmto zmenám sú aj súčasné moderné VSS považované za vysoko účinný bezpečnostný prvok. [9]

2.1 Základné časti dohľadových videosystémov

Dohľadovému videosystému sa neprisuduje iba funkcia pasívneho sledovania. Je od neho požadované, aby zachytené dáta boli prenášané do úložiska a na vizualizačné zariadenia, prípadne aby bol umožnený bezdrôtový prístup alebo boli vykonávané softvérové analýzy. Preto sa štandardná zostava skladá z týchto prvkov:

- **digitálne a analógové kamery** – kamery sú považované za základný prvok dohľadového videosystému. Aj keď sú analógové kamery v období digitalizácie postupne vyradované, vďaka ich schopnosti poskytovať kvalitné zábery si stále udržiavajú zastúpenie u ich výrobcov. Signál z kamery je zaznamenávaný v analógovej forme a najčastejšie sa prenáša koaxiálnym káblom, ktorého maximálna dĺžka je obmedzená na 100 metrov. Digitálne kamery sú definované ako zariadenia, ktorými je obraz zachytávaný a prostredníctvom počítačovej siete distribuovaný autorizovaným používateľom na sledovanie, správu a archiváciu videonahrávok. IP kamera je v podstate vnímaná ako samostatne fungujúci celok, v ktorom sú kamerové a počítačové funkcie integrované v jednom zariadení;
- **zdroj napájania** – bežné napájanie kamier je zabezpečované samostatnými káblami, pričom čoraz častejšie je využívaná technológia napájania cez ethernet (Power over Ethernet) ďalej už len ako PoE. Kamerám je štandardne dodávané napätie v rozmedzí

12 – 48 V. Napájacie jednotky môžu byť umiestňované v kovových krytoch s poistnými prvkami. K dispozícii sú aj verzie určené na inštaláciu do elektroinštalčných krabíc alebo rozvodných skriniek;

- **prenosová infraštruktúra** – prenosové trasy sú považované za dôležitú súčasť dohľadových videosystémov. Dáta z kamier sú nimi prenášané buď do úložiska, alebo na zobrazovacie zariadenia. Na prenos informácií sú využívané metalické vedenia, optické vlákna alebo bezdrôtové spojenia. Súčasťou týchto trás sú aj napájacie vedenia, prípadne vykurovacie obvody určené na vyhrievanie krytov kamier;
- **zobrazovacie a záznamové zariadenia** – záznam z kamier je zobrazovaný na monitoroch, tabletoch aj mobilných zariadeniach. Pre ukladanie videozáznamu boli s príchodom digitalizácie zavádzané digitálne videorekordéry ďalej už len ako DVR, ktorým bola postupne rozširovaná kapacita úložiska. Sieťový videorekordér (Network Video Recorder) ďalej už len ako NVR je digitálnym zariadením, s ktorým je komunikácia IP kamier zabezpečovaná pomocou pridelených IP adries;
- **krycie a montážne príslušenstvo** – kryty kamier sa zvyčajne inštalujú na ochranu zariadení alebo na ich maskovanie. Držiaky kamier musia disponovať dostatočnou nosnosťou a zároveň tlmiť otrasy a vibrácie. Na upevnenie kamier, ktoré je potrebné otáčať horizontálne aj vertikálne, sa používajú polohovacie hlavice. Ovládacia klávesnica je dnes realizovaná ako ovládací pult, ktorým dokážu byť prepájané všetky IP kamery;
- **doplňky** – ovládače, infračervené prislvielenie a ďalšie moduly, ako napríklad nočné videnie alebo vzdialené ovládanie, ktorými je funkčnosť systému rozširovaná.

Vo väčšine prípadov býva systém vybavený viacerými kamerami. Ich finálny počet je určovaný požiadavkami prevádzkovateľa a zložitou chráneného priestoru. [9]

V súlade s technickou normou ČSN EN 62676-1-1 sa dohľadové video systémy určené na bezpečnostné účely definujú ako ucelený súbor komponentov, ktorého hlavnými časťami sú kamery, záznamové jednotky, zobrazovacie a ovládacie zariadenia, ako aj komunikačné rozhrania. V norme sú stanovené základné systémové požiadavky na tieto prvky, pričom dôraz je kladený na ich vzájomnú kompatibilitu a funkčnú integritu v rámci jednotného systému. Taktiež sú v norme špecifikované úrovne účelu sledovania, ktoré sa rozdeľujú na detekciu, rozpoznanie a identifikáciu. Tieto úrovne sú určené na základe kvality

a rozlíšení obrazu v závislosti od vzdialenosti medzi kamerou a pozorovaným objektom. Takéto rozdelenie má zabezpečiť, aby bol dohľadový systém navrhnutý primerane konkrétnym bezpečnostným cieľom a požiadavkám na sledovanie. Norma zároveň kladie dôraz na vzájomnú kompatibilitu a jednotnosť technických rozhraní, čím sa zabezpečuje ich bezproblémové zapojenie do väčších systémových celkov alebo možnosť budúceho rozšírenia riešenia. Zohľadnenie požiadaviek tejto normy je preto nevyhnutné nielen pri výbere zariadení, ale aj pri samotnom návrhu celého systému dohľadu. [10]

2.2 Analógové kamery

Za analógovú bezpečnostnú kameru, je považované zariadenie, pri ktorom sa využíva tradičná analógová technológia na zber a prenos videozáznamu. Na rozdiel od digitálnych riešení sú zábery odosielané v analógovom formáte prostredníctvom koaxiálnych káblov do záznamového zariadenia, akým je digitálny videorekordér (Digital Video Recorder) ďalej už len ako DVR. Pri takejto kamere býva video najprv zachytené a následne konvertované na analógový signál, aby mohol byť zabezpečený plynulý prenos. [11]

2.2.1 Princíp činnosti analógových kamier

Za hlavný prínos analógových kamier je považovaná ich schopnosť prenášať obraz prostredníctvom analógového signálu. Záznam býva najprv vytvorený kamerovým snímačom a následne je konvertovaný na analógové impulzy tak, aby bol zabezpečený plynulý prenos po koaxiálnom vedení. Takýmto spôsobom je umožnené monitorovanie v reálnom čase. Bezpečnostné prúdy videa sú poskytované okamžite a spoľahlivo bez merateľnej latencie. Jednoduchá prevádzka medzi kamerou a zobrazovacím zariadením je vyzdvihovaná ako charakteristická výhoda analógového dohľadu, pretože je poskytovaný okamžitý a stabilný obraz sledovaného priestoru. [11]

Z technického hľadiska bývajú analógové kamery určené na zabezpečenie zložené z týchto častí, pričom všetky okrem skleného krytu a portov bývajú vnútri skrinky kamery:

- objektív;
- doska elektroniky (obvodová doska);
- sklenený kryt;
- vonkajší ochranný kryt;
- obrazový snímač;

- montážna konzola;
- napájacie konektory a koaxiálne porty.

Okrem samotnej kamery býva na inštaláciu potrebné zabezpečiť koaxiálny kábel a napájací adaptér. Na rozdiel od moderných IP kamier sú analógové viazané na pevné káblové pripojenie a nebýva umožnené ich bezdrôtové fungovanie. Montážna konzola je nevyhnutná na to, aby bolo zariadenie pevne uchytené na zvolenom mieste. [12]

2.2.2 Výhody analógových kamier

Aj napriek postupnému presunu trhu k digitálnym riešeniam si analógové kamery udržiavajú stabilné postavenie vďaka súboru praktických výhod z ktorých najdôležitejšie sú:

- **vysoká kvalita obrazu** – ostré a detailné snímky sú dosahované nasadením CCD snímača, ktorého vysoká svetelná citlivosť umožňuje zachytiť obraz aj pri slabom vonkajšom osvetlení alebo pri nočnom režime. Vďaka pokročilému spracovaniu signálu v DVR jednotke je následne každý snímok podrobený kompresii, pri ktorej sú uchované kľúčové vizuálne informácie bez viditeľnej degradácie. Takéto kompresné algoritmy optimalizujú veľkosť dát, pričom udržiavajú plynulý prenos obrazu aj pri obmedzenej šírke pásma. Výsledkom je vysoká prenosová rýchlosť, ktorá zabraňuje oneskoreniam či rozmazaniu pohybu v kritických momentoch sledovania;
- **bezpečný prenos snímok** – koaxiálne vedenie zabezpečuje priame a stabilné vedenie signálu nezávislé od zložitej počítačovej siete. Táto priamosť prenosovej cesty výrazne redukuje riziko výpadkov spôsobených sieťovým preťažením či chybami na úrovni smerovačov a prepínačov. Navyše, vďaka uzavretému charakteru tejto infraštruktúry nie je možné, aby vonkajšie elektromagnetické rušenie spôsobilo degradáciu kvality obrazu. Záznamy tak dorazia vždy úplné, bez prerušenia či straty dát;
- **vysoká bezpečnosť** – architektúra analógového systému je navrhnutá tak, aby bola odolná voči kybernetickým hrozbám. Kamery nevyužívajú IP protokol, a preto nie sú zraniteľné bežnými online útokmi, ako sú botnety, ransomvér či neautorizované sieťové skenovanie. Po stránke hardvéru sú dátové trasy izolované od zvyšku IT infraštruktúry, čo znemožňuje preniknutie škodlivého kódu do systému. Všetky

zaznamenané zábery sú uložené lokálne na DVR, kde sú chránené proti externým vplyvom aj fyzickou bezpečnosťou zariadenia;

- **udržiavateľnosť systému** – prevádzkovanie analógového kamerového systému je navrhnuté s dôrazom na jednoduchosť. Nevyžaduje sa konfigurácia IP adres, nastavenie sieťových protokolov ani inštalácia špecializovaného softvéru. Všetky základné operácie ako pripojenie kamier, alebo nastavenie parametrov obrazu, sú realizované priamo na DVR. Vďaka tomu môže byť systém udržiavaný aj všeobecným technikom bez pokročilých IT znalostí, čo znižuje náklady na servis a minimalizuje dobu nefunkčnosti pri bežnej údržbe;
- **dostupnosť inštalatérov a dodávateľov** – vzhľadom na dlhoročné rozšírenie analógových kamerových systémov na trhu je zabezpečené, že je k dispozícii široké spektrum firiem a špecialistov, ktorí sú kvalifikovaní na ich inštaláciu, konfiguráciu aj servis. V mnohých regiónoch sú služby dodávateľov a montážnych firiem bežne ponúkané, čo skracuje čakacie doby na realizáciu projektov a zjednodušuje proces výberu správneho partnera;
- **jednoduchosť prevádzky** – analógové zariadenia sú konštruované tak, aby bol proces prenosu videosignálu do DVR čo najpriamejší: video z kamier je v analógovej forme odovzdané priamo do záznamovej jednotky, kde sa automaticky vykoná digitalizácia, kompresia a archivácia. Vďaka tejto lineárnej architektúre sa eliminuje potreba komplexnej sieťovej konfigurácie, a tak sú inštalácia či rozšírenie systému zvládnutelné aj bez rozsiahlych IT znalostí. Celý proces je spravidla riadený cez jednoduché používateľské rozhranie DVR, ktoré umožňuje nastavenie nahrávania, prezeranie záznamov aj údržbu bez nutnosti inštalácie ďalšieho softvéru. [13; 14]

2.2.3 Nevýhody analógových kamier

Analógové kamery sú spojené so špecifickými obmedzeniami. Od náročnej elektroinštalácie a vysokých počiatočných nákladov, cez potrebu externých modulov v prípade rozšírenia funkcionality až po viazanosť kamier na pevné káblové pripojenie. Patria k tomu:

- **vysoké náklady na inštaláciu** – inštalácia analógového kamerového systému je charakterizovaná značnými počiatočnými investíciami. Každá kamera vyžaduje samostatné koaxiálne vedenie až k záznamovej jednotke, vrátane konektorov

a adaptérov, ktoré musia byť inštalované odborníkmi. Náklady na materiál ako je koaxiálny kábel, napájací zdroj, DVR aj prípadné rozbočovače, môžu v súčte prekročiť cenu moderného IP systému. Okrem toho je za každý meter kabeláže a za každú hodinu práce technika účtovaný poplatok, čo dokáže pri rozsiahlych inštaláciách navýšiť celkovú cenu aj o desiatky percent;

- **obmedzená ponuka moderných funkcií** – pokročilé analytické nástroje ako rozpoznávanie tvárí, detekcia neoprávneného vstupu či generovanie štatistík nie sú integrované priamo v kamere, ale je nutné ich dopĺňať externými servermi a softvérovými licenciami. Výsledkom je vyššia komplexnosť a náklady na rozšírenie inteligentných funkcií;
- **nutnosť pevného káblového pripojenia** – analógové kamery vyžadujú priame fyzické prepojenie ku záznamovej jednotke prostredníctvom koaxiálneho kábla. To v praxi znamená nutnosť viesť káble stropnými šachtami, podlahovými žľabmi alebo stenami, čo si vyžaduje stavebné úpravy a starostlivé plánovanie trás. V miestnostiach bez pripravených káblových trás sa často pristupuje k vŕtaniu, čo zvyšuje dobu inštalácie aj náklady na materiál a prácu;
- **obmedzená flexibilita inštalácie** – pri každom rozšírení či modifikácii systému ako je napríklad pridanie ďalšej kamery na nové miesto, musí byť vykonaná fyzická úprava existujúcich káblových trás a následné doladenie konfigurácie DVR jednotky. V dôsledku toho sa servisné zásahy predlžujú, pretože nie je možné jednoducho pridať či presunúť zariadenie pomocou softvérovej konfigurácie, ako je to u IP systémov. Prakticky každá takáto úprava si vyžaduje zásah kvalifikovaného technika, ktorý vykoná potrebné inštalátorské práce, skontroluje kvalitu signálu na novej trase a obnoví správne fungovanie záznamu. Z toho dôvodu je plánovanie zmien v analógových inštaláciách zložitejšie a pomalšie, čo u väčších projektov môže viesť k výrazným prestojom a vyšším servisným nákladom. [14; 15]

2.3 IP kamery

IP kamera je označovaná za digitálne bezpečnostné zariadenie, ktorému je priradená vlastná sieťová adresa. Záznam je prenášaný po zabezpečenej sieti alebo internete, takže je umožnené jeho vzdialené prezeranie na ľubovoľnom pripojenom zariadení. Lokálne DVR nie je vyžadované, pretože obraz je spracovávaný priamo v kamere a je zobrazovaný v reálnom čase. [16]

2.3.1 Princíp činnosti IP kamier

Obraz je zaznamenávaný rovnako ako pri analógovom CCTV, no následne digitalizovaný a je odosielaný buď bezdrôtovo, prostredníctvom Ethernetu alebo Univerzálnej Sériovej Zbernice (Universal Serial Bus) ďalej už len ako USB. Interný procesor kamery zabezpečuje kódovanie videa aj audia, takže externé spracovacie jednotky nie sú potrebné. Typické vlastnosti, ktoré sú IP kamerám prisudzované:

- **vzdialený dohľad** – sledovanie živého obrazu je umožnené prostredníctvom akéhokoľvek zabezpečeného smart zariadenia, pokiaľ používateľ disponuje príslušným oprávnením. Administrátorom a bezpečnostnému personálu je tak poskytovaný nepretržitý prístup k videozáznamom bez potreby fyzickej prítomnosti v mieste systému. Týmto spôsobom môže byť zabezpečená okamžitá reakcia na incidenty, zvýšená efektivita obsluhy a nepretržité pokrytie bezpečnostného dohľadu aj v iných lokalitách;
- **obojsmerná komunikácia** – nielen že sa umožňuje príjem zvukového signálu z monitorovaného priestoru, ale aj spätné vysielanie hlasovej informácie priamo prostredníctvom kamery. Táto funkcionality je obvykle implementovaná v zariadeniach vybavených vstavaným mikrofónom a reproduktorom, čím sa umožňuje priama obojsmerná komunikácia medzi operátorom a osobou pred kamerou. Takéto riešenie nachádza uplatnenie najmä pri vstupných kontrolách, v systémoch recepcnej správy alebo pri obsluhu vzdialených vstupných bodov;
- **redukovaná kabeláž** – technológia PoE umožňuje napájanie kamier a súčasný prenos dát prostredníctvom jediného Ethernetového kábla. V dôsledku toho je pri inštalácii eliminovaná potreba samostatného napájacieho vedenia, čím sa znižujú náklady na materiál aj čas potrebný na montáž. Táto architektúra zjednodušuje návrh systému a umožňuje flexibilnejšie pripojenie kamier v prostredí s obmedzenou elektroinštaláciou;
- **vysoké rozlíšenie** – v IP kamerových systémoch je bežne implementované zaznamenávanie videa vo vysokom rozlíšení, často v rozmedzí od HD až po 4K. Tým je zabezpečené detailné zachytenie sledovanej scény, čo umožňuje presnejšiu identifikáciu osôb, objektov alebo udalostí aj pri zväčšení obrazu. Vyššie rozlíšenie zároveň zvyšuje efektivitu následnej analýzy záznamov a podporuje využitie pokročilých softvérových nástrojov pre videoanalýtku. [16]

2.3.2 Bežné konfigurácie a typy IP kamier

IP kamery sú na trhu dostupné v rôznych technických a konštrukčných vyhotoveniach, ktoré umožňujú ich prispôsobenie konkrétnym požiadavkám monitorovaného prostredia. Jednotlivé typy sa odlišujú najmä možnosťami mechanického ovládania, spôsobom prenosu a napájania, ako aj flexibilitou nasadenia. Pri návrhu IP kamerového systému je preto potrebné zohľadniť charakter sledovaného priestoru, požiadavky na kvalitu obrazu, možnosti inštalácie a špecifiká prevádzkového prostredia. Práve z týchto dôvodov sú IP kamery rozlišované do niekoľkých bežných typov, ktoré sa uplatňujú podľa konkrétneho použitia. K týmto typom patria:

- **fixné IP kamery** – sú konštruované na nepretržité monitorovanie rizikových priestorov z pevne určenej pozorovacej polohy, pričom pri ich nasadení musí byť zohľadnený typ kamery a uhol záberu. V praxi sú valcovité kamery využívané pre sledovanie oblastí s požiadavkou na dlhší dosah a užšie zorné pole, zatiaľ čo kupolovité kamery sú nasadzované tam, kde je potrebné zabezpečiť širšie pokrytie pri kratšom dosahu. Medzi hlavné výhody týchto zariadení patrí nižšia spotreba prenosovej kapacity, ktorá umožňuje stabilnú a dlhodobú prevádzku systému. Fixné IP kamery sú inštalované v interiéroch aj exteriéroch, pričom svoje uplatnenie nachádzajú najmä v obchodných priestoroch, kanceláriách a prenajímaných objektoch;
- **Pan-Tilt-Zoom IP kamery** – otáčanie, naklápanie, približovanie (Pan-Tilt-Zoom) ďalej už len ako PTZ IP kamery sú vybavované pohyblivými objektívmi, ktorými je možné manipulovať v reálnom čase a teda môže byť menený uhol záberu otáčaním, naklápaním a priblížením. Týmto spôsobom je operátorovi umožnené aktívne sledovať dianie na diaľku. Táto funkcionálna však prispieva k vyššej spotrebe dátového prenosu a preto je vyžadovaná väčšia šírka pásma siete;
- **PoE IP kamery** – kamery s technológiou PoE sú konštruované tak, aby mohol byť napájací prúd aj dátový prenos vedený jedným Ethernetovým káblom. Na rozdiel od tradičných analógových riešení, pri ktorých sú inštalované dva samostatné káble a to napájací a signálny, je pri PoE systémoch dosahovaná jednoduchšia inštalácia a údržba, vďaka čomu sú znižované celkové technické nároky;
- **bezdrôtové IP kamery** – bezdrôtové IP kamery sú pripájané k súkromnej bezdrátovej internetovej sieti (Wireless Fidelity) ďalej už len ako Wi-Fi, aby mohli

odosielať videozáznam na väčšiu vzdialenosť. Záznam môže byť automaticky ukladaný do cloudového úložiska alebo na interné pamäťové médium, čo umožňuje plynulé zaznamenávanie bez prerušenia.

Tieto riešenia sú nasadzované najmä tam, kde je inštalácia ethernetovej kabeláže vyhodnotená ako náročná alebo neefektívna. Je však potrebné počítať s tým, že prenos dát cez bezdrôtovú sieť je vystavovaný rušeniu alebo kybernetickým útokom a preto nebýva odporúčaný pre vysoko zabezpečené prostredia bez pokročilého šifrovania. [14]

2.3.3 Výhody IP kamier

IP kamery predstavujú v súčasnosti štandardné riešenie sieťového video dohľadu. V porovnaní s analógovými systémami umožňuje ich digitálna architektúra jednoduchšiu integráciu do podnikového IT prostredia a otvára cestu k pokročilej analytike obrazu v reálnom čase. Vysoké rozlíšenie, flexibilné sieťové protokoly a podpora šifrovania zároveň rozširujú možnosti použitia od malých inštalácií až po rozsiahle siete. Vďaka napájaniu cez PoE a softvérovo riadenému nastavovaniu parametrov sa skracuje čas inštalácie a zjednodušuje údržba. Všetky tieto prednosti prispievajú k nižším prevádzkovým nákladom počas celého životného systému. Medzi najdôležitejšie výhody IP kamier patria:

- **nižšie náklady ako v minulosti** – počiatočné investície do IP kamier sú v súčasnosti výrazne nižšie než v minulosti, pričom cenová dostupnosť základných modelov je považovaná za priaznivú. Pri efektívnom návrhu systému je možné dosiahnuť rovnakú alebo vyššiu úroveň funkcionality s menším počtom IP kamier v porovnaní s analógovými riešeniami, čo prispieva k optimalizácii nákladov;
- **jednoduchšia inštalácia** – inštalácia IP kamier je zjednodušená vďaka využívaniu jedného ethernetového kábla, ktorý zabezpečuje súčasne prenos dát aj napájanie prostredníctvom technológie PoE. Oproti analógovým systémom, ktoré vyžadujú samostatné napájacie a signálne vedenie, je týmto spôsobom redukovaná komplexnosť kabeláže. Parametre ako ostrosť obrazu či zoom je možné nastavovať na diaľku prostredníctvom softvérovej správy bez potreby fyzického zásahu do inštalácie;
- **vyššie rozlíšenie** – záznam je štandardne zabezpečovaný vo vysokom rozlíšení. Bežne sú podporované rozlíšenia od Full HD, 4K a vyššie, čo umožňuje detailnú analýzu a presnú identifikáciu objektov v sledovanej scéne;

- **inteligentné funkcie a analytika** – moderné IP kamery sú vybavované integrovanými funkciami pokročilej analytiky obrazu, medzi ktoré patria detekcia pohybu, detekcia dymu, počítanie osôb, sledovanie farebných prvkov, definovanie zón a automatické generovanie výstrah. Tieto funkcie sú implementované priamo v zariadení, bez potreby nasadzovania dodatočných hardvérových alebo softvérových modulov, čím sa zvyšuje efektivita spracovania dát a znižuje časová odozva systému;
- **otvorená platforma** – IP kamery sú navrhované ako otvorené systémy, čo umožňuje ich bezproblémovú integráciu s rôznymi typmi video management softvéru a iných bezpečnostných riešení. Vďaka štandardizovaným protokolom je zabezpečená vysoká kompatibilita, čo uľahčuje budúce rozširovanie systému alebo prechod na nové technológie bez nutnosti výmeny existujúcich komponentov. [14]

2.3.4 Nevýhody IP kamier

Implementácia IP videotechniky je sprevádzaná viacerými obmedzeniami, ktoré musia byť zohľadnené ešte pred samotnou migráciou z analógového systému. V technickom návrhu sa vyžaduje prepočítanie kapacity úložísk, priepustnosti sietí aj potrebného školenia obsluhy, aby bola zachovaná prevádzková spoľahlivosť. Náklady spojené s kúpou nových zariadení a výmenou infraštruktúry môžu pri prvotnej investícii výrazne zaťažiť rozpočet. Aj po uvedení do prevádzky je nevyhnutné počítať s vyššími dátovými nárokmi, ktoré sa premietajú do priebežných nákladov na úložisko. Medzi najvýznamnejšie nevýhody IP kamier patria:

- **vyššie počiatkové náklady pri prechode z analógového systému** – pri prechode z existujúceho analógového systému na IP technológiu je potrebné počítať s vyššou počiatkovou investíciou. Výmena zastaranej infraštruktúry vrátane kamerových zariadení, záznamových serverov, aktívnych sieťových prvkov a kabeláže si vyžaduje značné finančné prostriedky. Okrem toho je často nutné zabezpečiť kompatibilitu nových komponentov so zvyškom podnikového IT prostredia, čo môže vyvolať dodatočné náklady na integráciu a konfiguráciu systému;
- **nároky na úložisko** – záznam vo vysokom rozlíšení, ktorý je pre IP kamery charakteristický, vedie k tvorbe veľkého objemu dát. V dôsledku toho je potrebné zabezpečiť adekvátnu kapacitu úložiska a optimalizovať archiváciu. Bez dostatočne dimenzovaného úložiska môže dôjsť k obmedzeniu doby uchovania dát alebo k strate starších záznamov. Pri rozsiahlych inštaláciách je nevyhnutné pravidelne prehodnocovať

a prispôsobovať architektúru dátových úložísk tak, aby boli pokryté rastúce požiadavky na kapacitu;

- **potrebná znalosť rozhrania** – ovládanie a správa IP kamerového systému je vykonávaná prostredníctvom softvérového rozhrania, ktoré musí byť správne zvládnuté koncovými používateľmi. Niektoré pokročilé funkcie a konfiguračné možnosti si vyžadujú odborné školenie personálu, aby bola zabezpečená optimálna a bezchybná prevádzka systému. Nedostatočná znalosť rozhrania môže viesť k neefektívnemu využívaniu dostupných funkcií alebo k chybám pri konfigurácii a správe systému. [14]

2.3.5 Odporúčania pri prechode na IP systém

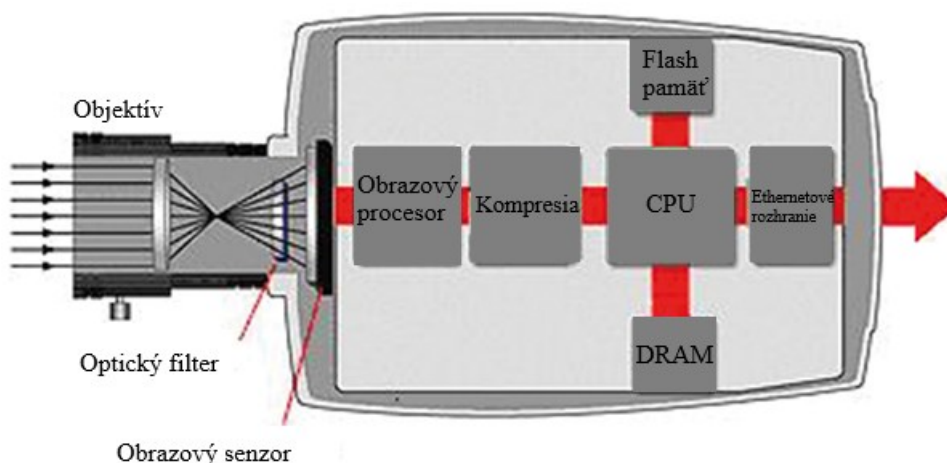
Pred samotným prechodom z analógového na IP kamerový systém sa má vypracovať stručný postup, ktorý zohľadní technické limity súčasnej infraštruktúry, finančné možnosti investora a očakávanú úroveň rizika. V prípravnej fázy by mali byť preverené svetelné podmienky, kapacita siete aj dostupnosť úložiska, aby sa predišlo neskorším nákladným úpravám. Implementácia sa odporúča rozdeliť na etapy, čím sa umožní priebežné testovanie funkčnosti a optimalizácia rozpočtu. Na základe týchto východísk sa odporúča dodržať nasledujúce kroky:

- **zapojiť nezávislého poradcu** – pred začatím implementácie má byť zabezpečená odborná konzultácia. Očakávania od nového systému majú byť zosúladené s jeho reálnymi technickými možnosťami a s podmienkami v konkrétnom objekte. Nezávislému poradcovi má byť umožnené objektívne vyhodnotiť potreby prevádzky a navrhnúť optimálne riešenie;
- **zohľadniť svetelné podmienky** – pri návrhu systému má byť vykonaná analýza osvetlenia monitorovaných priestorov, nakoľko nevhodné alebo nevyrovnané svetelné podmienky môžu mať negatívny vplyv na kvalitu obrazu a efektivitu záznamu;
- **postupná výmena** – v prípade obmedzeného rozpočtu sa odporúča zavádzanie IP kamier realizovať postupne, pričom prioritne majú byť vybavené najrizikovejšie alebo najdôležitejšie monitorované oblasti;
- **vybrať odborného dodávateľa** – inštalácia a konfigurácia systému by mala byť zverená dodávateľovi so skúsenosťami v oblasti IP videotechniky a sieťových riešení. Odborný partner má byť schopný zabezpečiť optimálne nastavenie systému, jeho integráciu s existujúcou infraštruktúrou a zaškolenie obsluhy;

- **stanoviť realistické ciele a potreby** – funkcie a rozsah systému majú byť navrhnuté v súlade so skutočnými prevádzkovými potrebami. Pri plánovaní má byť zohľadnený dostupný rozpočet, účel využitia a požadovaná trvácnosť riešenia. Odporúča sa vyhnúť sa implementácii nadbytočných alebo neefektívnych funkcií, ktoré by mohli systém zbytočne predražiť alebo skomplikovať jeho správu;
- **revidovať bezpečnostný plán** – v rámci prechodu na IP technológiu má byť vykonaná revízia celého kamerového systému. Má byť zhodnotené pokrytie priestorov, vhodnosť umiestnenia jednotlivých kamier a celková miera súladu systému s aktuálnymi rizikami a potrebami prevádzky;
- **navrhnuť systém s ohľadom na budúci rast** – systém má byť od začiatku navrhnutý s ohľadom na budúcu rozširiteľnosť. Je potrebné počítať s tým, že požiadavka na doplnenie ďalších kamier alebo rozšírenie funkčnosti býva po uvedení systému do prevádzky veľmi častá;
- **navštíviť podobné objekty** – skúsenosti z reálnej prevádzky majú byť overené prostredníctvom návštevy referenčných objektov s podobným systémom. Informácie získané priamo od používateľov môžu napomôcť pri optimalizácii návrhu a výbere najvhodnejších riešení;
- **vypracovať písomnú stratégiu a pravidlá** – v rámci projektovej dokumentácie má byť vypracovaná jasná a preukázateľná stratégia správy systému. V nej majú byť definované pravidlá údržby, rozpočtové rámce, zásady uchovávanía záznamov, pravidlá prístupu k videu a konkrétny účel využívania systému. Dôsledné spracovanie týchto dokumentov prispieva k dlhodobej udržateľnosti a transparentnosti prevádzky systému. [14]

2.4 Optické prvky kamier

Za hranicu, ktorá je v rámci blokovej štruktúry kamery vnímaná ako prechod medzi optickými prvkami a časťou určenou na spracovanie elektrického signálu, je považovaný obrazový senzor. Z hľadiska časového postupu snímania obrazu sú rozlišované dve hlavné časti a to objektív a obrazový senzor. Prostredníctvom objektívu je žiarenie odrazené od snímaného objektu sústredené a zaostrené na povrch obrazového senzora. Na tomto senzore je dopadajúce žiarenie konvertované na elektrický signál, ktorý je následne spracovávaný v ďalších častiach kamerového systému. [9]



Obrázok 1 Bloková schéma kamery

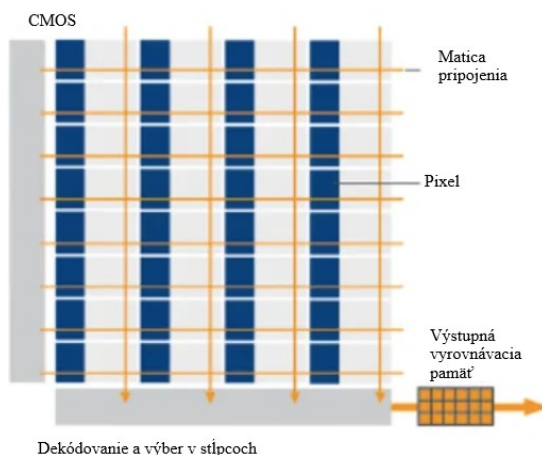
(upravené z: [17])

2.4.1 Obrazový senzor

V prevažnej väčšine kamier dohľadových video systémov sú používané dva základné typy obrazových senzorov a to komplementárny kov-oxidový polovodič (Complementary Metal-Oxide Semiconductor) ďalej už len ako CMOS a zariadenie s nábojovou väzbou (Charge-Coupled Device) ďalej už len ako CCD. Oba typy snímačov sú vytvárané z množstva jednotlivých obrazových bodov a to pixelov, ktorým je priradovaná funkcia zachytávať dopadajúce fotóny svetla. Rozdiel medzi oboma typmi je daný technológiou výroby a spôsobom vyčítavania informácií z jednotlivých pixelov.

1. CMOS senzory

CMOS senzory sú tvorené mriežkou snímacích buniek, ktoré sú usporiadané pravidelne a sú citlivé na dopadajúce svetlo. Ich výroba je uskutočňovaná rovnakým technologickým procesom ako pri bežných integrovaných obvodoch, čo umožňuje nižšie náklady a vyššiu integráciu funkcií. Každá snímacia bunka je vybavená vlastným analógovo-digitálnym, ďalej už len ako A/D prevodníkom a zosilňovačom, čo znamená, že digitalizácia obrazu je realizovaná priamo na úrovni každého pixelu. Tento prístup vedie k zníženiu energetickej spotreby a zrýchľuje spracovanie obrazu, pretože údaje sú vyčítavané paralelne. Signál z každého pixelu je následne spracovávaný pomocou tranzistorového zapojenia. Vyčítanie pixelov je zabezpečované riadkovým a stĺpcovým dekodérom, pričom frekvencia vyčítavania dosahuje jednotky až stovky megahertzov. Jednotlivé pixely sú zostavené z fotodiódy, ktorá mení dopadajúce svetlo na elektrický náboj a tranzistorov, ktoré slúžia na zosilnenie signálu, výber pixelu a jeho resetovanie pred ďalším snímaním. [9]

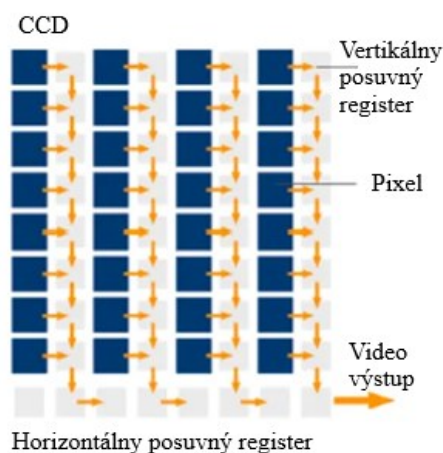


Obrázok 2 Princíp CMOS snímača

(upravené z: [18])

2. CCD senzory

CCD senzory sú založené na fotoelektrickom jave. Dopadajúce svetlo je konvertované na elektrický náboj v jednotlivých snímacích bunkách. Získaný signál je následne presúvaný cez jednotlivé bunky až na okraj snímača, kde je vložený do takzvaného posuvného registra. Tento register odovzdáva signál do zosilňovača a A/D prevodníka, ktoré sú umiestnené mimo samotného senzora. CCD snímače registrujú iba intenzitu dopadajúceho svetla. Ak má byť rozlíšená farba, sú na senzor aplikované červené, zelené, modré (Red–Green–Blue) ďalej už len ako RGB filtre. Tieto senzory sú využívané najmä v špecializovaných kamerách ako napríklad v zariadeniach pre režim noc/deň, pri slabom osvetlení (low–light) alebo pre infračervené spektrum. [9]



Obrázok 3 Princíp CCD snímača

(upravené z: [18])

2.4.2 Objektív

Objektív je považovaný za neoddeliteľnú a prevažne samostatnú súčasť kamery, prostredníctvom ktorej je ovplyvňovaná kvalita výsledného obrazu. Správnu voľbou a nastavením technických parametrov objektívu môže byť zásadne ovplyvnené zorné pole, úroveň detailnosti, hĺbka ostrosti, ako aj schopnosť kamery monitorovania pri slabom osvetlení. Z hľadiska klasifikácie sú objektívy rozdeľované do troch hlavných skupín:

- **fixné objektívy** – fixné objektívy (s pevnou ohniskovou vzdialenosťou) sú konštruované na jedno konkrétne a nemeniteľné nastavenie ohniska. Sú využívané tam, kde kamera zostáva inštalovaná v nemennom uhle a rozsah sledovania sa nemení. Vďaka jednoduchosti je umožnená spoľahlivá prevádzka bez potreby dodatočného nastavovania;
- **varifokálne objektívy** – varifokálne objektívy sú vybavené možnosťou meniť ohniskovú vzdialenosť v určitom rozsahu. Každá zmena nastavenia si vyžaduje ručný zásah priamo na kamere, vrátane úpravy clony a zaostrenia. Po nakonfigurovaní požadovaného uhla záberu je monitorovaná oblasť definovaná pevne. Varifokálne objektívy sú označované rozsahom ohniskovej vzdialenosti, svetlosťou a kompatibilnou veľkosťou obrazového snímača;
- **zoom objektívy** – zoom objektívy sú charakterizované premenlivou ohniskovou vzdialenosťou, podobne ako varifokálne, no ich nastavenie nie je ovplyvňované manuálnym zásahom a tak sú zmeny ohniska vykonávané

automaticky alebo na diaľku. Vo väčšine prípadov sú tieto objektívy vybavované servomotormi, ktoré umožňujú nastavovanie priblíženia bez fyzického zásahu. Sú nasadzované najmä v prípade PTZ kamier alebo tam, kde je požadované dynamické sledovanie rôznych častí scény. Zoom objektívy, rovnako ako varifokálne, sú označované rozsahom priblíženia, rozsahom clony a kompatibilitou s veľkosťou snímača. [9]

2.5 Faktory ovplyvňujúce VSS

Implementácia video dohľadových systémov býva vnímaná ako zásadná investícia, ktorá spoločnostiam umožňuje udržať si konkurenčný náskok. Zákazníci zvyknú nadobúdať väčší pocit dôvery, ak je prostredie organizácie vybavené rozsiahlym kamerovým dohľadom. Preto sa odporúča, aby boli prizvaný špecialisti na video dohľad, vďaka ktorým môže byť využitá ich strategická expertíza pri plánovaní bezpečnosti. Konzultuje sa s nimi, ktoré technológie sú kľúčové pre špecifické potreby danej firmy. V odvetviach s vyššie hodnoteným rizikom, napríklad vo financiách či regulovanom prostredí, musia byť často nasadzované ešte prepracovanejšie riešenia. Pri zvažovaní vhodného kamerového systému je nutné prihliadať na kľúčové faktory, ktorých dôsledným posúdením môže byť dosiahnutá najvyššia možná kvalita monitorovania bez toho, aby boli ohrozené náklady alebo škálovateľnosť riešenia. [19]

Pred samotným obstaraním kamerového systému má byť zohľadnených niekoľko kľúčových faktorov a to:

1. inštalácia

- musí byť posúdená finančná náročnosť montáže, najmä ak majú byť vybavené viaceré prevádzky s členitou architektúrou;
- býva vyžadované dodatočné hardvérové vybavenie, softvér či kabeláž;

2. cena

- okrem počiatočnej investície musí byť dopočítaná aj celková cena vlastníctva;
- náklady na prevádzku a uchovávanie záznamov môžu ovplyvniť výslednú sumu;

3. typ kamery

- analógová technológia bola dlhé roky používaná ako jediná voľba;

- v súčasnosti sú nasadzované IP kamery, ktorým sú umožňované funkcie ako automatické poplachy pri detekcii pohybu či video analytika. Pôvodné analógové riešenia sú nahrádzané modernejšou platformou;

4. typ úložiska

- systémy sú klasifikované na NVR, DVR a hybridné verzie;
- DVR býva spájaný s analógovými kamerami, zatiaľ čo NVR je uprednostňovaný pri IP zariadeniach, keďže je obohatený o rozšírené sieťové funkcie;
- hybridné prevedenie je vytvárané tam, kde je potrebné podporiť oba druhy kamier;

5. súbor funkcií

- k dispozícii sú ponúkané rôzne technológie, napríklad PTZ ovládanie, nočné videnie, PoE napájanie, rozlíšenie 8K a podobne;

6. požiadavky na monitorovanie

- spôsob a intenzita dohľadu bývajú považované za jeden z najdôležitejších determinujúcich prvkov pri prispôbovaní video dohľadového riešenia; [20]

7. hĺbka ostrosti

- pri ochrane rozličných kategórií majetku je považovaná hĺbka ostrosti za kľúčový parameter. Ak má byť monitorovaný logistický sklad spolu s kancelárskymi miestami, má byť zvolené riešenie, ktorým je zachytávaná čo najväčšia plocha pri najmenšom počte kamier. Keďže kamery nemôžu byť rozmiestnené na každom mieste, musí byť zabezpečené širšie zorné pole. Sú preferované zariadenia, ktorými je snímaný kvalitný obraz na veľkú vzdialenosť bez toho, aby bola vyžadovaná značná montážna plocha. Nové objektívové technológie sú využívané na hlbšiu integráciu dohľadu do administratívnych priestorov. Moderné kamery sú navrhované s možnosťou digitálneho priblíženia či záznamu v rozlíšení Full HD. Tieto funkcie môžu byť uplatňované iba vtedy, keď sú nasadzované systémy vyššej kvalitatívnej triedy. Z toho dôvodu býva optimalizovaná kvalita optiky, prenosových kanálov a monitorovacieho panelu, aby bola dosiahnutá maximálna hĺbka ostrosti;

8. dohľad v cloude

- využitím cloud computingu bola rozšírená dostupnosť bezpečnostných riešení pre širší okruh zákazníkov. Kamery môžu byť prepojené so skladmi, kanceláriami aj regionálnymi pobočkami pri nižších obstarávacích nákladoch a sú podporované konkurenčné služby. V oblasti cloudového video dohľadu sú vyvíjané produkty, ktoré využívajú sieťovú infraštruktúru na nepretržitý dohľad. Pretože lokálne dátové centrum nie je inštalované, nie je možné, aby bolo fyzicky napadnuté alebo poškodené. Cloudová architektúra zároveň zvyšuje odolnosť voči vzdialeným útokom. Tradičné systémy bývali kompromitované prostredníctvom serverových zraniteľností, čo umožňovalo útočníkom dlhodobé sledovanie. Pri cloudovom riešení je budovaná silnejšia ochranná zóna okolo celého dohľadového ekosystému;

9. pokročilá integrácia dohľadu

- v prostrediach s vyššími bezpečnostnými nárokmi sú uprednostňované aktívne, umelou inteligenciou podporované kamery pred pasívnymi systémami. Pohyb v objekte je sledovaný algoritmami, anomálie sú identifikované v reálnom čase a rozsiahle metadáta sú ukladané na ďalšie spracovanie. Analytické nástroje sú často začleňované priamo do kamerovej platformy. Strojové učenie je aplikované na vyťaženie cenných poznatkov a na posilnenie ochrany. Okrem obrazu sú zapájané aj zariadenia internetu vecí (Internet of Things) ďalej už len ako IoT, ktorými sú zbierané doplnkové údaje. Operátori môžu byť informovaní, kedy bol sprístupnený konkrétny priestor a ako dlho ostali ponechané otvorené dvere do úsekov s najvyšším stupňom zabezpečenia. [19]

2.5.1 Vlastnosti moderného systému

V súčasnosti sú nasadzované viaceré technológie, ktoré z kamerového systému robia proaktívne riešenie:

- je umožňovaný vzdialený prístup zo smartfónov, tabletov či notebookov;
- sú implementované video analytické algoritmy a rozpoznávanie tvárí;
- ceny hardvéru boli znížené natoľko, že systémy sú sprístupňované širokému okruhu domácností.

Na výber vhodných zariadení, býva odporúčané, aby bol oslovený bezpečnostný špecialista, ktorý vie identifikovať špecifické riziká každého objektu. [20]

2.5.2 Kľúčové faktory pri rozhodovaní

Pri výbere optimálnej videotechniky sú zvyčajne posudzované nasledujúce aspekty:

1. býva zvažovaná možnosť vzdialeného monitorovania. Obrazové toky sú odosielané DVR alebo priamo do cloudu, odkiaľ sú sprístupňované oprávneným používateľom;
2. sú ponúkané služby diaľkového stráženia, v rámci ktorých je zabezpečovaný 24 hodinový dohľad profesionálmi. V prípade narušenia býva kontaktovaná polícia;
3. externé kamery sú nainštalované na kritických miestach, napríklad pred garážou, pri sklade alebo pri zadnom vchode do objektu, aby bola zaručená identifikácia osôb ešte pred vstupom do objektu;
4. prístupové dvere môžu byť ovládané na diaľku pričom návšteva býva rozpoznaná kamerou a vstup je umožnený prostredníctvom aplikácie. [20]

2.6 Konkrétne kamery

V tejto časti sú uvedené vybrané modely kamier, ktoré zahŕňajú základné aj pokročilé funkcie. Pre každý z modelov sú prezentované kľúčové technické parametre, ktoré ovplyvňujú investičné aj prevádzkové náklady a predpokladanú životnosť zariadenia. Ku každej kamere je priložená sekcia s technickými údajmi a poznámkami, ktoré vysvetľujú ako dané parametre prispievajú k výpočtu TCO.

2.6.1 AXIS M1045-LW

Model AXIS M1045-LW je definovaný ako vnútorná bezdrôtová IP kamera, ktorej obraz je snímaný 1/3 palcovým CMOS senzorom a je poskytovaný v rozlíšení Full HD 1080p pri 30 snímkach za sekundu. Vďaka mechanickému infračervenému (Infra Red) ďalej už len ako IR-cut filtru a vstavaným infračerveným elektroluminiscenčným diódam (Light-Emitting Diode) ďalej už len ako LED svetlám je zabezpečená nepretržitá prevádzka vo dne i v noci. Minimálna citlivosť je udávaná na 0,25 lux (farebne) a 0,05 lux (čierno-bielo), pričom pri zapnutom prísветení je dosahované 0 lux. Obraz je komprimovaný kodekom H.264 s technológiou Zipstream, ktorá znižuje dátový tok bez straty podstatných detailov a je ukladaný buď do sieťového úložiska, alebo priamo na microSD kartu. Bezdrôtová komunikácia je realizovaná cez Wi-Fi a alternatívne je umožnené pripojenie cez 100 Mb/s

portu lokálnej siete (Local Area Network) ďalej už len ako LAN. Kamera je dodávaná s držiakom pre stenu a roh, ktorým je uľahčená montáž. Horizontálny uhol záberu dosahuje približne 110°. Pri typickej prevádzke je odoberaných okolo 2,7 W, maximálne 4,4 W. [21]

Tabuľka 2 Technické parametre kamery AXIS M1045-LW

Parameter	Hodnota (datasheet)	Poznámka pre TCO
Senzor	1/3" CMOS	Integrovaný A/D prevodník – nižšia spotreba
Rozlíšenie / FPS	1920 × 1080 px @ 30 fps	Full HD zvyšuje nároky na úložisko
Objektív	2,8 mm, F/2.0	Pevná ohnisková vzdialenosť
Zorné pole (H/V)	110 ° / 61 °	Pokryje malú miestnosť jednou kamerou
Nočný režim	IR-cut + LED (dosah 10 m)	0 lux pri zapnutom IR
Kompresia	H.264, MJPEG + Zipstream	Šetrí šírku pásma a kapacitu disku
Ukladanie	microSD / microSDHC / NAS	Edge storage znižuje záťaž siete
Konektivita	Wi-Fi 2,4 & 5 GHz, 10/100 LAN	Flexibilná inštalácia bez PoE
Spotreba	typ. 2,7 W, max 4,4 W	Dôležité pre prevádzkové náklady
Prevádzka	0 °C – 40 °C, 10 – 85 % RH	Vhodné pre bežné interiéry
Rozmery / hmotnosť	106 × 60 × 37 mm / 126 g	Kompaktné vyhotovenie
Analytika	MotionGuard, FenceGuard, LoiteringGuard	Znižuje náklady na dohľad
Záruka	5 rokov	Vplýva na LCC/TCO

(upravené z: [21])

V tabuľke 2 sú v súlade s bežnou praxou v oblasti IP videotechniky použité viaceré technické skratky. Pre zabezpečenie terminologickej konzistencie v rámci celej práce je v tabuľke 3 uvedená ich vysvetľujúca legenda. Tieto skratky budú následne v práci používané v jednotnej forme vo všetkých častiach.

Tabuľka 3 Legenda skratiek z tabuľky 2

Skratka	Anglický názov	Slovenský názov
FPS	Frames Per Second	Počet snímok za sekundu
px	Pixel	Pixel
MJPEG	Motion Joint Photographic Experts Group	Motion Joint Photographic Experts Group
SD	Secure Digital	Typ úložiska
SDHC	Secure Digital High Capacity	Rozšírenie SD formátu pre vyššie kapacity
NAS	Network Attached Storage	Sieťové úložisko
GHz	GigaHertz	GigaHertz
W	Watt	Watt
RH	Relative Humidity	Relatívna Vlhkosť
mm	MiliMeter	MiliMeter
g	Gram	Gram

(zdroj: vlastný)

2.6.2 AXIS Q1635

Kamera AXIS Q1635 je prezentovaná ako profesionálne vnútorné IP zariadenie určené na precízne sledovanie rýchlych scén v náročných svetelných podmienkach. Obraz je snímávaný 1/2 palcovým progresívnym CMOS senzorom a je poskytovaný v rozlíšení HDTV 1080p pri 50 / 60 fps, takže detail rýchlo pohybujúcich sa objektov je zachytávaný bez rozmazania. Funkcie Wide Dynamic Range, Forensic Capture a Lightfinder sú využívané na zvýraznenie detailov v kontrastných scénach a pri slabom osvetlení, zatiaľ čo elektronická stabilizácia obrazu vyhladzuje vibrácie a konštrukcie. Video stream je optimalizovaný technológiou Zipstream. Kamera je napájaná cez PoE alebo jednosmerným napätím 8 – 28 V DC a typická spotreba dosahuje približne 8 W. [22]

Tabuľka 4 Technické parametre kamery AXIS Q1635

Parameter	Hodnota (datasheet)	Poznámka pre TCO
Senzor	1/3" CMOS, progresívny scan	Väčší snímač - vyššia citlivosť, lepší nočný obraz
Rozlíšenie / FPS	1920 x 1080 px @ 50/60 fps	Vyššia snímková frekvencia - zvýšená kapacita úložiska
Objektív	Varifokál 4 – 13 mm, P-iris	Flexibilné nastavenie uhla záberu
Zorné pole (H/V)	102° – 33° / variabilné	Určuje počet kamier potrebných na pokrytie priestoru
Minimálne osvetlenie	0,1 lux (farba), 0,01 lux (Č/B)	Dôležité pre nočný režim bez IR osvetlenia
IR prisvietenie	Externé voliteľné	Vplyv na dodatočnú spotrebu/príslušenstvo
Špeciálne funkcie	WDR 120 dB, Lightfinder, EIS	Znižujú riziko nekvalitného záznamu - nižšie náklady na opakované zásahy
Kompresia	H.264 + Zipstream, MJPEG	Priamy dopad na šírku pásma a veľkosť archívu
Multi-view streaming	Až 8 vyrezaných scén	Šetrí počet kamier v systéme
Analytika	Video Motion Detection, aktiv. tampering, audio detekcia	Môže znižovať potrebu dodatočného softvéru
Napájanie	PoE IEEE 802.3af / 8 – 28 V DC	Flexibilná inštalácia, spotreba maximálne 8 W
Úložisko	micro SD / NAS s AES šifrovaním	Edge storage znižuje sieťovú záťaž
Prevádzkové prostredie	0 °C – 55 °C, 10 – 85 % RH	Určuje vhodnosť pre interiér / chránený exteriér
Hmotnosť	0,94 kg	Vplyv na typ držiaka a montážne náklady
Záruka	3 roky (s možnosťou rozšírenia)	Faktor pri kalkulácii LCC/TCO

(upravené z: [22])

V tabuľke 4 sa v súlade s normami a výrobcom používa viacero odborných skratiek. Pre zabezpečenie terminologickej jednotnosti v ďalšom texte práce sú tieto skratky uvedené v Tabuľke 5. Skratky budú následne používané v práci v jednotnej forme.

Tabuľka 5 Legenda skratiek z Tabuľky 4

Skratka	Anglický názov	Slovenský názov
Č/B	Black / White	Čierno / Biela
dB	decibel	decibel
IEEE	Institute of Electrical and Electronics Engineers	Inštitút elektrotechnických a elektronických inžinierov
af	Auto Focus	Automatické zaostrovanie
V	Volt	Volt
DC	Direct Current	Jednosmerný prúd
AES	Advanced Encryption Standard	Pokročilý štandard šifrovania
°C	Degrees Celsius	Stupne Celzia
kg	KiloGram	KiloGram

(zdroj: vlastný)

2.6.3 AXIS P1435-LE

Kamera AXIS P1435-LE je charakterizovaná ako kompaktné vonkajšie zariadenie určené na nepretržité snímanie v náročných svetelných podmienkach. Vďaka funkciám Lightfinder a „široký dynamický rozsah“ (Wide Dynamic Range) ďalej už len ako WDR – Forensic Capture je dosahovaná vysoká kvalita obraz v rozlíšení HDTV 1080p pri 50 / 60 fps. Integrované LED diódy s technológiou Optimized IR zabezpečujú prispôsobenie expozície pri minimálnom osvetlení, čím sú eliminované šumy v nočnom režime. Objektív s varifokálnym rozsahom je vybavený diaľkovým zaostrovaním a zoomom, ovládaným prostredníctvom webového rozhrania. P-Iris riadenie udržiava optimálnu hĺbku ostrosti a kontrast. Video je komprimované kodekom H.264, pričom Zipstream znižuje dátový tok aj kapacitu archívu. Kamera je osadená IP66 / IP67 a NEMA 4X puzdrom, ktoré je dimenzované na teploty -30 °C až +55 °C. Napájanie je zabezpečované cez PoE s typickým odberom 4,6 W. [23]

Tabuľka 6 Technické parametre kamery AXIS P1435-LE

Parameter	Hodnota (datasheet)	Poznámka pre TCO
Senzor	1/2.8" CMOS (progresívny scan)	Cítlivosť pri nízkom osvetlení
Rozlíšenie / FPS	1920 × 1080 @ 50 / 60 fps (bez WDR)	Nároky na šírku pásma a úložisko
Objektív (variant A)	3 – 10,5 mm, F 1.4, HFOV 95° – 35°	Široký záber – menej kamier v systéme
Objektív (variant B)	10 – 22 mm, F 1.85, HFOV 34,5° – 18°	Detailné sledovanie vzdialených cieľov
IR prísветlenie	Optimized IR, dosah 30 m / 50 m	Nočný dohľad bez externých reflektorov
Min. osvetlenie (3–10,5 mm)	0,12 lux (farba) / 0,01 lux (Č/B)	Určuje použiteľnosť pri tlmenom osvetlení
Krytie	IP66 / IP67 / NEMA 4X / IK08	Náklady na kryté inštalácie - minimalizované
Kompresia	H.264 (High/Main/Baseline) + Zipstream	Úspora dátového toku ≈ 30 – 50 %
Analytika	Motion/Fence/Loitering Guard, VMD	Znižuje potrebu manuálneho dohľadu
Úložisko	microSD/SDHC/SDXC + NAS, šifrovanie	Edge storage šetrí sieťové zdroje
Napájanie	PoE 802.3af / at, typ. 4,6 W	Priamo ovplyvňuje prevádzkové náklady
Prevádzka	–30 °C ... +55 °C, 10 – 100 % RH	Bez nutnosti vyhrievaného krytu
Rozmery / hmotnosť	Ø 132 × 260 mm / 800 g	Vplýva na typ držiaka a montáž
Záruka	3 roky (s možnosťou rozšírenia)	Faktor pri dlhodobých nákladoch (LCC)

(upravené z: [23])

V tabuľke 6 sa používajú odborné skratky, ktoré sa v dokumentácií výrobcov považujú za štandardné. Pre zabezpečenie terminologickej konzistencie v ďalšom texte práce sú tieto skratky uvedené a vysvetlené v tabuľke 7. Skratky budú následne používané v celom texte práce v jednotnej forme.

Tabuľka 7 Legenda skratiek z Tabuľky 6

Skratka	Anglický názov	Slovenský názov
HFOV	Horizontal Field Of View	Horizontálny zorný uhol
NEMA	National Electrical Manufacturers Association	Americká norma pre krytie zariadení
IK	Impact Protection Rating (IK Code)	Trieda mechanickej odolnosti proti nárazu
VMD	Video Motion Detection	Detekcia pohybu vo videu
SDXC	Secure Digital eXtended Capacity	Rozšírený formát SD karty s vysokou kapacitou

(zdroj: vlastný)

2.6.4 AXIS P3225-LVE Mk II

Kamera AXIS P3225-LVE Mk II je predstavovaná ako kompaktná fixná dómová jednotka, ktorá je dimenzovaná na vonkajšiu prevádzku a poskytuje video v rozlíšení HDTV 1080p. Vďaka funkciám Lightfinder a WDR – Forensic Capture je dosahovaná vysoká kvalita obrazu aj pri silných svetelných kontrastoch. Vstavané LED diódy s technológiou Optimized IR zabezpečujú nepretržité snímanie pri nulovom osvetlení. Objektív s rozsahom 3 – 10,5 mm je vybavený diaľkovým zoomom a zaostrovaním, pričom P-Iris riadenia udržiava optimálnu hĺbku ostrosti. Video je komprimované v kodeku H.264 a je optimalizované technológiou Zipstream, ktorá znižuje šírku pásma a veľkosť archívu. Robustné puzdro spĺňa triedu IP66/67 a IK10, takže kamera je chránená pred poveternostnými vplyvmi i vandalizmom. Napájanie je realizované cez PoE a typickým odberom 7,3 W. [24]

Tabuľka 8 Technické parametre kamery AXIS P3225-LVE Mk II

Parameter	Hodnota (datasheet)	Vzťah k TCO / dôvod sledovania
Senzor	1/3" CMOS (progresívny scan)	Citlivosť pri slabom osvetlení
Rozlíšenie / FPS	1920 × 1080 px @ 25/30 fps (WDR) / 50/60 fps (bez WDR)	Vyššia snímková frekvencia - väčší dátový tok
Objektív	Varifokál 3 – 10,5 mm, F 1.4, HFOV 92° – 34°	Flexibilné pokrytie scény
Min. osvetlenie	0,16 lux (farba) / 0,03 lux (Č/B)	Určuje potrebu dodatočného osvetlenia
IR prísivlenie	Optimized IR, dosah do 30 m	Nočný dohľad bez externých reflektorov
WDR	Až 120 dB	Znižuje riziko nepoužiteľných záberov
Krytie / Odolnosť	IP66/67, NEMA 4X, IK10	Vplyv na dlhodobú životnosť
Kompresia	H.264 (High/Main/Baseline) + Zipstream	Šetrí šírku pásma a úložisko
Analytika	Motion/Fence/Loitering Guard, VMD	Znižuje potrebu ručného dohľadu
Ukladanie	microSD/SDHC/SDXC + NAS, šifrovanie	Edge storage odľahčuje sieť
Napájanie	PoE IEEE 802.3af/at, max 10,8 W	Priamo vplýva na energetické náklady
Prevádzka	–40 °C až +50 °C, 10 – 100 % RH	Eliminuje potrebu vyhrievacieho krytu
Rozmery / hmotnosť	Ø 149 × 104 mm / 0,8 kg	Určuje montážne príslušenstvo
Záruka	3 roky (s možnosťou predĺženia)	Faktor pri LCC/TCO

(upravené z: [24])

V tabuľke 8 je použitá skratka EIS, ktorá je v oblasti video dohľadu štandardne používaná. Pre zabezpečenie terminologickej jednotnosti v práci je táto skratka vysvetlená v tabuľke 9 a bude v texte používaná v jednotnej forme.

Tabuľka 9 Legenda skratiek z Tabuľky 8

Skratka	Anglický názov	Slovenský názov
EIS	Electronic Image Stabilization	Elektronická stabilizácia obrazu

(zdroj: vlastný)

2.6.5 AXIS Q3505-V

Kamera AXIS Q3505-V je prezentovaná ako vnútorná dómová jednotka, ktorá poskytuje video v rozlíšení HDTV 1080p pri až 60 fps. Vďaka funkcií WDR – Forensic Capture je optimalizovaný kontrast scén s extrémnymi rozdielmi jasu, zatiaľ čo technológia

Lightfinder zabezpečuje vysokú citlivosť pri slabom osvetlení. Systém dokáže plynule prechádzať medzi režimom WDR a nočným režimom bez straty detailov. Elektronická stabilizácia obrazu (EIS) eliminuje vibrácie montážnej konštrukcie a prispieva k plynulejšiemu záznamu. Objektív s varifokálnym rozsahom je vybavený diaľkovým zaostrovaním a zoomom. Prostredníctvom P-Iris riadenia je udržiavaná optimálna hĺbka ostrosti. Videostream je komprimovaný v kodeku H.264 a je optimalizovaný technológiou Zipstream, ktorá znižuje dátový tok a kapacitu archívu. Krytie IK10 spolu s ochranou IP52 chráni kameru pred vandalizmom a prachom. Napájanie je zabezpečované cez PoE s maximálnym odberom približne 5,5 W. [25]

Tabuľka 10 Technické parametre kamery AXIS Q3505-V

Parameter	Hodnota (datasheet)	Dôvod sledovania / vplyv na TCO
Senzor	1/2.8" CMOS, progresívny scan	Citlivosť pri nízkom osvetlení
Rozlíšenie / FPS	1920 × 1080 px @ 60 fps (bez WDR) / 30 fps (s WDR)	Vyššie fps - väčší dátový tok
Objektív – model 9 mm	3 – 9 mm, F 1.3, HFOV 105° – 35°	Širšie pokrytie scény
Objektív – model 22 mm	9 – 22 mm, F 1.6, HFOV 33° – 16°	Detailné sledovanie vzdialených miest
Min. osvetlenie (9 mm)	0,18 lux (farba) / 0,04 lux (Č/B)	Potreba doplnkového osvetlenia
WDR	Až 120 dB	Znižuje riziko nepoužiteľných záberov
Stabilizácia	Elektronická (EIS)	Nížšie skryté náklady pri vibráciách
Krytie / odolnosť	IP52, IK10	Predlžuje životnosť, znižuje servis
Kompresia	H.264 + Zipstream, MJPEG	Šetrí šírku pásma a úložisko
Analytika	VMD, tampering, audio detekcia	Menej manuálneho dohľadu
Ukladanie	SD/SDHC/SDXC + NAS	Edge storage odľahčuje sieť
Napájanie	PoE 802.3af/at, max 5,5 W	Priamy vplyv na prevádzkové náklady
Prevádzka	-10 °C až +50 °C	Vhodné pre väčšinu interiérov
Rozmery / hmotnosť	Ø 149 mm × v 104 mm / 1,2 kg	Určuje typ montáže
Záruka	3 roky (možnosť predĺženia)	Faktor pri LCC/TCO

(upravené z: [25])

3 POPLACHOVÉ ZABEZPEČOVACIE A TIESŇOVÉ SYSTÉMY

Poplachové zabezpečovacie a tiesňové systémy, ktoré boli v minulosti označované ako elektrická zabezpečovacia signalizácia, ďalej už len ako EZS, sú definované ako technický súbor zariadení určený na ochranu objektov pred neoprávneným vniknutím. Včasnou detekciou narušenia a prenosom poplachovej informácie na obsluhu systému je umožnené minimalizovať rozsah materiálnych, prípadne aj osobných škôd. Zabezpečovací systém býva tvorený centrálnou riadiacou jednotkou, takzvanou ústredňou, ku ktorej sú pripojené ovládacie prvky ako napríklad klávesnica slúžiaca na zapnutie a vypnutie systému. Súčasťou systému bývajú aj detekčné senzory, vnútorné alebo vonkajšie, ktoré sledujú monitorovaný priestor a výstupné zariadenia, ktorými je používateľ informovaný o narušení, napríklad sirénami alebo telefonickými komunikátormi. V prípade potreby môže byť systém prepojený s pultom centralizovanej ochrany, ďalej už len ako PCO, ktorého prevádzka je zaisťovaná nepretržitou obsluhou bezpečnostnej služby, polície alebo súkromnej strážnej agentúry.

Tieto zabezpečovacie systémy môžu fungovať ako samostatné riešenie, no zároveň bývajú často integrované do iných bezpečnostných technológií. Môže ísť napríklad o prístupové systémy, kde sú vstupy ovládané prostredníctvom kariet, čipov alebo biometrických údajov, o perimetrickú ochranu prostredníctvom infračervených závor, prípadne o prepojenie s kamerovými systémami. Funkčnosť zabezpečovacích systémov je možné ďalej rozšíriť o ďalšie detekčné prvky, akými sú elektronické požiarne hlásiče, detektory úniku plynov, záplavové snímače či otrasové detektory. Tieto zariadenia sú navrhnuté tak, aby dokázali včas identifikovať potenciálne havárie alebo požiare a informovať obsluhu systému o ich vzniku. Vďaka tomu je možné efektívne predchádzať škodám na majetku, zdraví alebo dokonca životoch osôb. [26]

V súlade s normou ČSN EN 50131-1 ed. 2:2007 sa od poplachových zabezpečovacích a tiesňových systémov vyžaduje, aby boli zatriedené do príslušnej bezpečnostnej triedy (Grade 1 – Grade 4) na základe úrovne rizika chráneného objektu. Súčasne má byť každému zariadeniu priradená klimatická kategória I až IV, čím sa určí rozsah prípustnej teploty a vlhkosti. V norme je ďalej predpísané, že poplachový signál musí byť vygenerovaný do 30 sekúnd od detekcie a sabotážne stavy musia byť zaznamenané najneskôr do 100 sekúnd. Komunikačný kanál má byť nepretržite monitorovaný a každý prenos poplachu má byť potvrdený spätnou väzbou. Požaduje sa aj redundantné napájanie, plná prevádzka má byť akumulátorovou zálohou zabezpečená minimálne 12 hodín pri Grade 2 a 24 hodín pri Grade 3 a 4 a vedenia musia byť chránené pred skratom i prerušením. Norma taktiež

ukladá povinnosť archivovať všetky udalosti s časovou pečiatkou počas najmenej 30 dní, pričom prístup k záznamom má byť zaznamenávaný. Dodržaním týchto systémových požiadaviek sa zaručuje jednotná kvalita, overiteľnosť a spoľahlivosť PZTS. [27]

3.1 Prvky PZTS

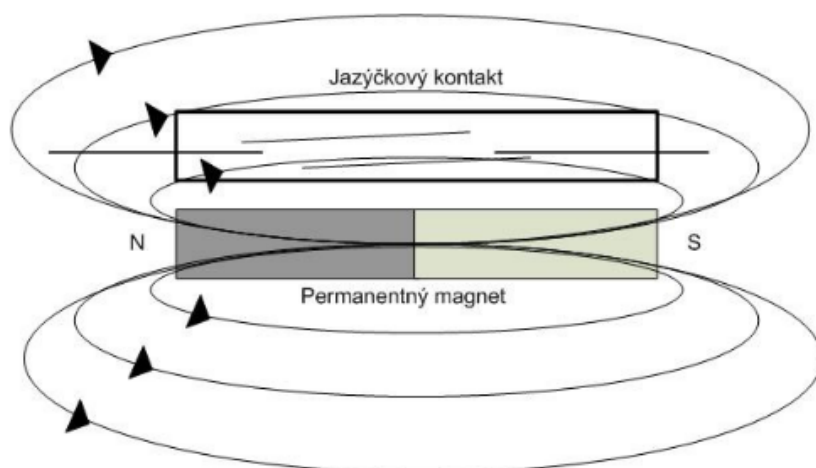
Jednotlivé prvky PZTS sú rozdeľované do viacerých kategórií podľa typu chráneného priestoru. Patria sem prvky plášťovej, priestorovej, predmetovej, perimetrickej ochrany a prvky tiesňového hlásenia. [28]

3.1.1 Prvky plášťovej ochrany

Ich úlohou je zabezpečiť kontrolu a ochranu prienikov cez obvodové konštrukcie budovy, ako sú okná, dvere, brány či iné vstupné otvory. Tieto prvky sú určené najmä na detekciu otvorenia alebo poškodenia stavebných častí. [28; 29]

1. Magnetické kontakty

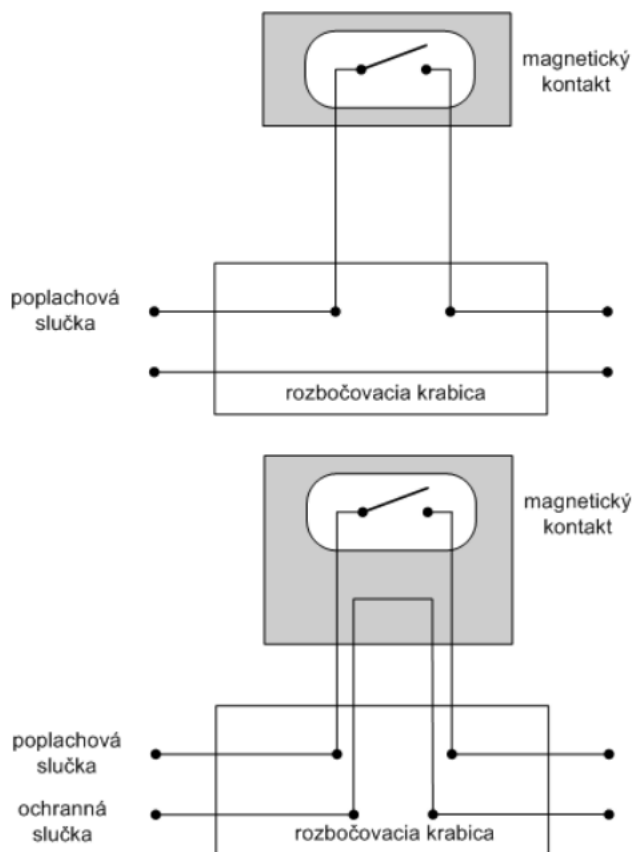
Magnetické kontakty sú považované za pasívne čidlá určené na detekciu neoprávneného otvorenia prvkov ako sú okná, dvere, brány a podobne. Vždy sú konštruované ako dvojdielne zariadenie, pozostávajúce z jazýčkového kontaktu a permanentného magnetu. Jazýčkový kontakt je umiestnený v hermeticky uzavretej sklenej trubici naplnenej ochrannou atmosférou, v ktorej sú zakotvené dve pružné feromagnetické kontakty. Permanentný magnet je najčastejšie vyhotovený z feritového materiálu vo forme valčeka a je umiestnený tak, aby jeho magnetické pole udržiavalo kontakty v zopnutom stave. Keď je magnet odtiahnutý nad dovolenú hranicu teda typicky pri otvorení okna alebo dverí, magnetické pole zoslabne a kontakty sa samovoľne rozpoja, čo je systémom vyhodnotené ako poplachová udalosť. [28; 29]



Obrázok 4 Princíp funkcie magnetického kontaktu

(zdroj: [29])

Obe časti bývajú zapuzdrené v krytoch z nemagnetického materiálu ako je odolný plast alebo hliníková zliatina, čím sa zabezpečí mechanická i klimatická odolnosť. Pre skrytú montáž sú časti integrované priamo do rámu stavebného prvku. pre náročnejšie aplikácie ako napríklad rolety alebo priemyselné prostredie sa používajú robustné verzie odolné voči vonkajším vplyvom a aj proti cudzím magnetickým poliam. U niektorých typov sa pre zvýšenie úrovne zabezpečenia používajú viaceré jazýčkové kontakty zapojené buď sériovo alebo paralelne, prípadne je samotný kontakt polarizovaný. Elektrické pripojenie sa vykonáva do poplachovej slučky ústredne, buď v jednoduchom prevedení bez ochrannej slučky, alebo s doplnkovou ochrannou slučkou, ktorá detekuje pokus o odpojenie či manipuláciu s čidlom. [28; 29]



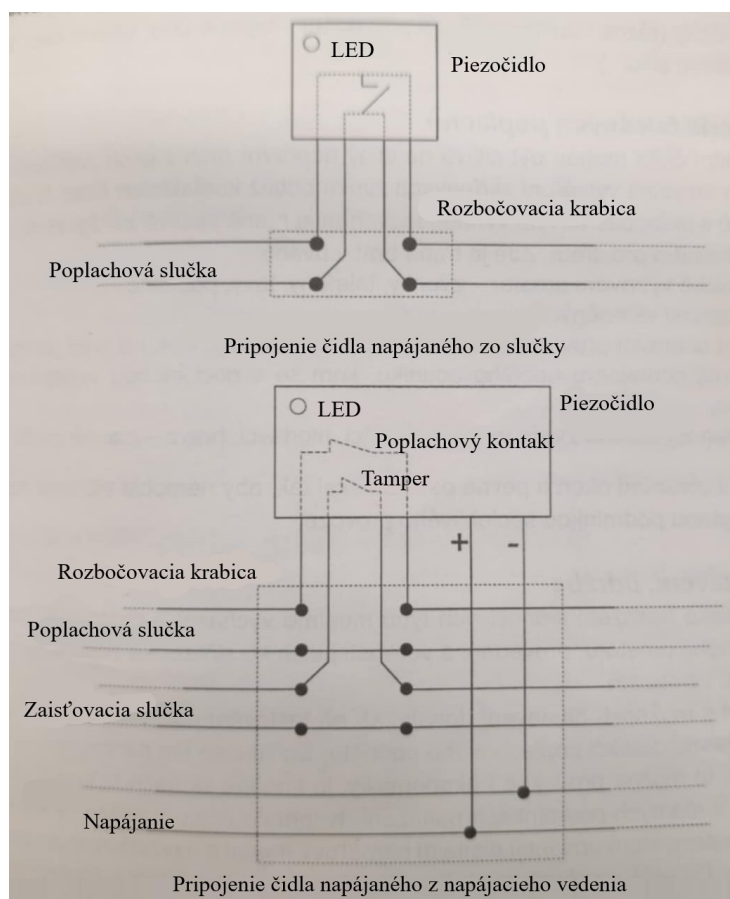
Obrázok 5 Schéma elektrického pripojenia magnetických kontaktov

(zdroj: [29])

Montáž sa realizuje tak, že magnet je upevnený na pohyblivú časť ako je krídlo okna alebo dverí a jazýčkový kontakt na rám. Pri inštalácii sa musí dodržať výrobcom stanovená maximálna aj minimálna vzdialenosť medzi čidlom a magnetom, správna orientácia magnetu a použitie výhradne nemagnetických upevňovacích prvkov. U rámov vyrobených z magnetických materiálov sa musia použiť špeciálne kontakty alebo podložky z nemagnetického materiálu podľa odporúčanej hrúbky. Vodiče sa vedú skryto v elektroinštalačných trubkách alebo lištách až do rozbočovacej krabice. Magnetické kontakty sú považované za veľmi spoľahlivé čidlá s dlhou životnosťou a minimom mechanických častí. Falošné poplachy sú zvyčajne spôsobené nedodržaním montážnych pokynov, nesprávnym dosadením okien či dverí alebo ich nesprávnym zabezpečením. Správne fungovanie je po montáži overené meraním odporu v poplachovej slučke pomocou digitálneho multimetra a kontrolou integrity okruhu. Najčastejšími závadami sú mechanické poškodenie tenkého prívodného kábla pri montáži, uvoľnenie krytu alebo čiastočná demagnetizácia permanentného magnetu. [28; 29]

2. Senzory na ochranu sklenených plôch

Čidlá na ochranu sklenených plôch sú určené na včasnú detekciu mechanického poškodenia alebo rozbitia skla. Pri rozbití skla sa vyvolá charakteristické vlnové kmitanie, ktoré je zachytené čidlom pevne pripevneným na povrchu skla. Pritom sa kladie dôraz na minimalizáciu strát pri prenose zvuku. Po narušení skla sú vzniknuté vibrácie elektronicky spracované a vyhodnotené ako poplachový signál. V závislosti od typu čidla je buď rozopnutý bezpotenciálový kontakt relé zapojený do poplachovej slučky, alebo je zaznamenaný prudký nárast odberu prúdu napájacej slučky. Dosah kontaktných čidiel sa pohybuje v rozmedzí približne 1,5 až 3 m. [28; 29]



Obrázok 6 Elektrické pripojenie čidiel na ochranu sklenených plôch

(upravené z: [28])

Kontaktné čidlá staršieho prevedenia obsahovali jednoduchý pružinový prvok, ktorého aktivácia bola závislá od priameho poškodenia skla a posunu telesa čidla. Pre zvýšenú úroveň rizík boli vyvinuté aktívne čidlá, v ktorých sa meranie zmeny prenosu zvukových vln porovnávalo s referenčnou hodnotou uloženou v pamäti. Tieto čidlá dokázali strážiť

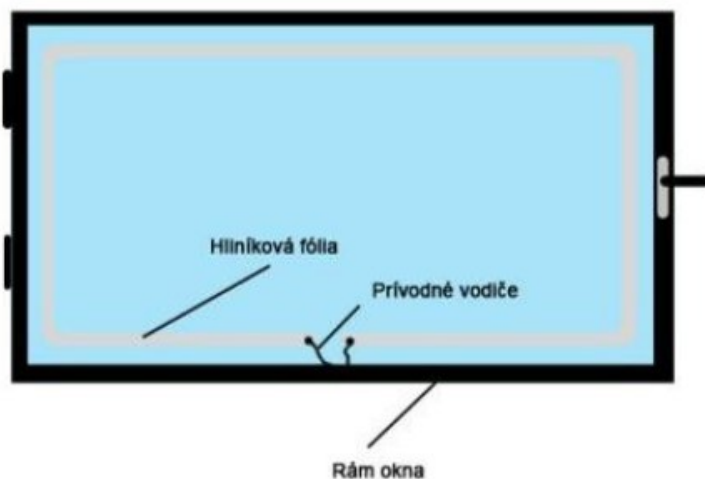
plochu až do vzdialenosti 25 m podľa typu skla. V praxi sa najčastejšie uplatnili akustické čidlá rozbitia skla, v ktorých je zachytený frekvenčný priebeh trieštenia skla. Pokročilé modely overujú prítomnosť viacerých úzkych frekvenčných pásiem súčasne, čím sa znižuje počet planých poplachov. Najnovšie verzie analyzujú vybrané diskkrétne frekvenčné body a poplach je vyvolaný až po potvrdení všetkých požadovaných kmitočtových zložiek v stanovenom časovom okne. Pri montáži kontaktných čidiel sa dbá na zachovanie odstupu približne 50 mm od rámu sklenej plochy a ich upevnenie v dolnej časti so smerovaním kábla nadol, aby bolo porušenie spoja okamžite viditeľné. Pred lepením sa sklo dôkladne odmastí a použijú sa lepidlá. Jedno kontaktné čidlo je schopné monitorovať len jednu samostatnú presklenú plochu, čo viedlo k preferencii akustických variantov pre ich jednoduchšiu inštaláciu a pokrytie väčších plôch. Za hlavné zdroje planých poplachov je považovaný silný okolitý hluk od napríklad dopravných prostriedkov, zvončeky, elektronika, zámerné vytváranie škripavých zvukov pri skle alebo vibrácie prenášané konštrukciou budovy. U akustických čidiel je navyše potrebné zohľadniť možné tlmenie zvuku závesmi, žalúziami či bezpečnostnými fóliami, ktoré môžu znižovať citlivosť detekcie. Nastavenie citlivosti čidiel s regulovateľným dosahom spočíva v zvolení minimálneho dosahu, pri ktorom je ešte spoľahlivo zaznamenaná poplachová udalosť, čím sa obmedzí náchylnosť na plané poplachy. Funkcia sa overuje buď jednoduchým poklepaním kovovým predmetom v mieste určenom výrobcom, alebo pomocou špeciálnych testerov s nahrávkou zvuku rozbíjajúceho sa skla. Čidlá sa považujú za bez údržbové, no pri zistení zníženej funkčnosti alebo mechanického poškodenia sa vyžaduje výmena celého modulu. [28; 29]

3. Poplachové fólie, tapety, nálepky a bezpečnostné sklá

Poplachové fólie, tapety, nálepky a bezpečnostné sklá sú čidlá, ktoré sú založené na princípe prerušenia vodivého materiálu. Vnútri nosiča ako sú fólie, tapety alebo sklá býva umiestnený tenký drôt alebo pásik vodivej fólie, ktorý je prilepený na povrch stráženej plochy. Keď je tento vodič prerušený napríklad prelomením drôtička pri vniknutí, vyhodnotí sa poplach. Polepy sú historicky známe ako najčastejšie používaná viditeľná forma ochrany presklenných plôch výkladných skriniek a okien. V súčasnosti sú však často opomínané, hoci si plošné aplikácie vzoru meandra, čo je vodivý vzor vlnovitej čiary, na vnútornej strane dverí vstupu do stráženého priestoru zaslúžia zvýšenú pozornosť. Pri ich montáži sa pripojovací bod vždy umiestňuje k hornej hrane plochy tak, aby bol chránený pred kondenzáciou pary, ktorá by mohla znížiť životnosť a spoľahlivosť spojenia. Zároveň sa však v objektoch, ktoré majú okná a dvere so sklenými výplňami prejavila potreba

vyvinúť čidlá, ktoré by zabránili vniknutiu cez tieto presklené plochy. Na tento účel boli vyvinuté detektory rozbitia skla, ktoré sa delia na tri základné typy:

- **kontaktné snímače** – sú navrhované tak, že je na obvod sklenenej plochy nanesený pás vodivej hliníkovej fólie, ktorou je vytvorený uzavretý elektrický obvod. Pred nanesením sa sklo dôkladne odmastí, aby sa zaistilo rovnomerné priľnutie fólie a dlhodobá spoľahlivosť vodivej dráhy. Fólia je obvykle prilepená buď pozdĺž okraja skla, alebo v tvare meandrovitého vzoru, čím sa dosiahne prekrytie celej stráženej plochy. Elektrické prírodné vodiče sú schované v drážkach rámu tak, aby bolo zložitejšie ich presne lokalizovať a prepojiť. Po mechanickom poškodení skla dôjde k priamemu prerušeniu vodivej fólie, čím sa rozpojí obvod a poplach je vyhodnotený ústredňou systémom. Táto metóda je rýchlo a jednoducho realizovateľná, no považuje sa za zraniteľnú voči cieľenej manipulácii. Pri presnom vyrezaní skla môže byť systém obídený bez spustenia poplachu. Z tohto dôvodu sú kontaktné snímače najčastejšie používané na výkladových sklách obchodov alebo ako sekundárna úroveň ochrany v objektoch s nižším bezpečnostným rizikom;

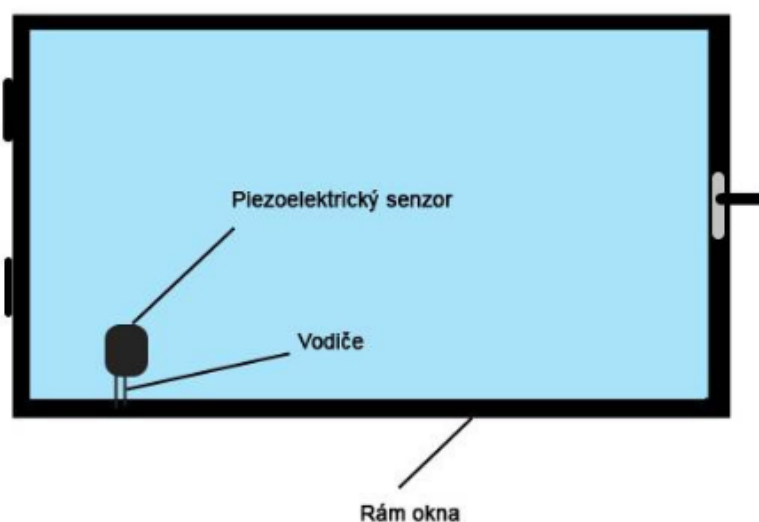


Obrázok 7 Spôsob umiestnenia kontaktných snímačov

(zdroj: [29])

- **piezoelektrické snímače** – fungujú na princípe premeny mechanických otrasov skla na elektrický signál. Na povrch skla je v rohu pripevnený tenký plátok piezoelektrického kryštálu, ktorý pri náraze alebo reze skla vyvolá vznik elektrického napätia. Tento signál sa odovzdá do riadiacej a vyhodnocovacej jednotky, kde je porovnaný s uloženými vzorkami charakteristických impulzov

z rozbitia. V prípade zhody je vyhlásený poplach. Dosah takto inštalovaných snímačov sa pohybuje v rozmedzí 1,5 až 5 metrov, pričom ich umiestnenie v rohu skla zabezpečuje optimálny prenos otrasových vln. Aby sa minimalizovalo riziko planých poplachov, prispôsobuje sa citlivosť každého snímača podľa reálnych prevádzkových podmienok;



Obrázok 8 Spôsob umiestnenia piezoelektrického snímača

(zdroj: [29])

- **akustické detektory rozbitia skla** – sú založené na detekcii charakteristického zvuku trieštenia skla pomocou mikrofónu. Prijatý akustický signál je filtrovaný tak, aby boli zachytené frekvencie typické pre rozbitie skla. Kvalitné modely zároveň vyhodnocujú prítomnosť viacerých frekvenčných zložiek súčasne, čím sa znižuje šanca na falošné poplachy, napríklad v dôsledku zvonenia telefónu či zvukov z vonkajšieho prostredia. Moderné verzie pracujú v duálnom režime keďže rozbitie skla sprevádza nielen zvuk trieštenia, ale vyhodnocujú aj zmenu tlaku v miestnosti. Poplach vyhlásený až vtedy, keď sa v tom istom čase zaznamená zmena tlaku aj typický akustický signál. Takto inštalované detektory sa umiestňujú na stenu kolmú k chránenej presklenej ploche a ich dosah môže dosiahnuť až 10 metrov od sklenenej tabule;



Obrázok 9 Akustický
detektor rozbitia skla

(zdroj: [29])

- **aktívne detektory rozbitia skla** – sú postavené na princípe vysielania ultrazvukových alebo infračervených impulzov a následného vyhodnocovania ich odrazov. Vysielač vysielá ultrazvuk, ktorý sa odráža od okolia skla a prijímač porovnáva prijatý odrazený signál s uloženou referenciou „zdravého“ odrazu. V prípade, že je prijatý signál odlišný, je systémom vyhodnotený ako poplach. Napriek tomu, že každý z týchto typov detektorov dokáže spoľahlivo signalizovať rozbitie sklenenej výplne, je potrebné pri ich aplikácii počítat s vysokou náročnosťou ručnej práce pri realizácii všetkých variantov ochrany plášťa objektu. [28; 29]

3.1.2 Prvky priestorovej ochrany

Priestorová ochrana bola vyvinutá ako účinné doplnenie k plášťovej ochrane, umožňujúce detekciu neoprávneného vniknutia priamo do interiéru stráženého priestoru. Priestorové čidlá sa rozoznávajú na pasívne a aktívne typy podľa spôsobu detekcie narušenia. Pasívne čidlá pri zisťovaní charakteristických znakov narušenia iba registrujú fyzikálne zmeny vo svojom okolí bez toho, aby vytvárali vlastné pracovné pole. Na druhej strane aktívne čidlá svoje pracovné prostredie najprv aktivujú vlastným signálom a potom merajú zmenu tohto vytvoreného poľa spôsobenú prítomnosťou osoby v priestore. V praxi sa pasívne aj aktívne

princípy často kombinujú v rámci jedného zariadenia, aby sa dosiahla vyššia spoľahlivosť a nižšia náchylnosť na plané poplachy. [28; 29]

1. Pasívne infračervené detektory

Pasívne infračervené (Passive Infrared) ďalej už len ako PIR detektory sú navrhované na vyhodnocovanie zmien vyžarovania v oblasti infračerveného spektra elektromagnetického žiarenia. V ich konštrukcii sa nachádza pyroelektrický senzor, ktorý dokáže zaznamenať odlišnosti infračerveného žiarenia dopadajúceho na tento detekčný prvok. K vyhláseniu zmeny stavu dochádza len vtedy, keď sa v zornom poli senzora pohybuje objekt s inou teplotou, než je teplota okolitého prostredia. Po detekcii tejto anomálie je nasledujúcou elektronickou časťou generované poplachové hlásenie. Vzhľadom na svoju jednoduchú konštrukciu sú tieto detektory veľmi rozšírené. Ich popularita spočíva predovšetkým v tom, že na detekciu pohybu človeka nie je potrebné vlastné vysielanie elektromagnetického žiarenia, ako je tomu v prípade mikrovlnných senzorov. Základ PIR detektora tvoria viaceré komponenty. Pyroelektrický senzor, vyrobený z dielektrika, je zvyčajne uložený v kovovom puzdre s priehľadným okienkom, umožňujúcim prienik infračerveného žiarenia k aktívnej časti snímača. Keď dochádza k absorpcii tepelnej energie, v dielektriku sa vytvára povrchový elektrický náboj, ktorý vyvoláva zmenu jeho polarizácie a následne sa prejavuje ako elektrické napätie. Na zosilnenie a spracovanie týchto signálov slúži predzosilňovač, ktorý je často integrovaný v tom istom puzdre spolu s dvoma alebo viacerými senzorovými prvkami s cieľom zvýšiť spoľahlivosť detekcie.

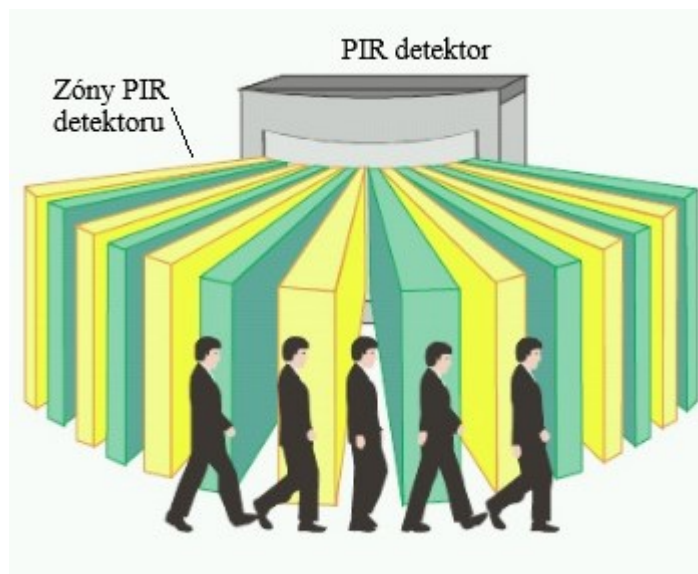
Optická sústava PIR detektora je zvyčajne tvorená buď radou fresnelových šošoviek, alebo členeným parabolickým zrkadlom. Tieto prvky zabezpečujú, že infračervené žiarenie z celej detekčnej zóny bude sústredené na pyroelektrický senzor rovnomerným spôsobom. Elektronika, ktorá sleduje signály zo senzora, obsahuje obvody na filtrovanie šumu, nastavenie citlivosti a vyhodnocovanie charakteru zachytených pulzov infračerveného žiarenia. Súčasťou modulov býva aj tamper kontakt, ktorým sa zaznamená akýkoľvek pokus o manipuláciu s puzdrom detektora, a indikačné LED prvky, ktoré vizuálne signalizujú aktuálny stav zariadenia. Doplnkové obvody sa potom starajú o stabilizáciu napájania, ochranu proti prepätiu a ďalšie servisné funkcie. [28; 29]



Obrázok 10 Konštrukcia PIR detektora

(upravené z: [29])

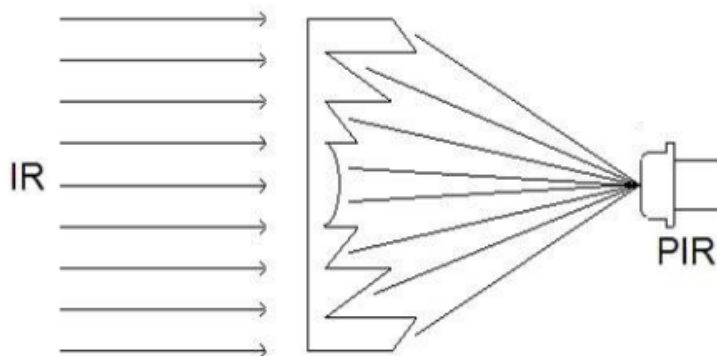
Statický zdroj infračerveného žiarenia nemôže byť týmito detektormi zachytený, preto sú PIR detektory využívané výlučne na detekciu pohybu. Pri konštrukcii zariadenia s pyroelektrickým senzorom býva použitý špeciálny optický systém, ktorého úlohou je zosilniť signál a zvýšiť citlivosť rozdelením detekčnej oblasti na viacero samostatných zón. Každá zo zón pokrýva časť priestoru, a ak sa pohybujúci sa objekt v priestore presúva z jednej zóny do druhej, jeho prítomnosť sa deteguje. Najvyššia citlivosť detektora je dosahovaná vtedy, keď sa objekt pohybuje kolmo na optickú os PIR snímača. Ak sa však objekt pohybuje priamo k čidlu alebo od neho, citlivosť značne klesá, a preto sa zorné pole rozdeľuje aj vo vertikálnom smere, aby sa podobné pohyby zachytili rovnakou spoľahlivosťou. [28; 29]



Obrázok 11 Zóny PIR detektoru

(upravené z: [29])

Optické systémy PIR detektorov sú zvyčajne zložené zo sústav šošoviek alebo sústav lomených zrkadiel. V prípade šošovkových riešení sú do priestoru detektora osadené hlavne stupňovité Fresnelove šošovky, ktoré sa vyrábajú prevažne z plastických materiálov. Tieto šošovky sú konštruované z viacerých tenkých priehľadných a nepriehľadných prstencov usporiadaných okolo spoločného stredu na jednej priehľadnej ploche. Pri ich osadení je možné zabezpečiť, aby sa pyroelektrický senzor umiestnil presne v ohnisku každej z týchto prstencových šošoviek. Vďaka rozdeleniu celej plochy na sústavu prstencových členov dochádza k tomu, že dopadajúce infračervené žiarenie zo širokej oblasti priestoru je prostredníctvom jednotlivých priehľadných prstencov postupne usmerňované a sústred'ované presne na snímacu plochu senzora. Týmto spôsobom je zabezpečené maximálne zosilnenie aj pomerne slabých infračervených signálov vyžarovaných pohybujúcimi sa objektmi, čím sa dosahuje vysoká citlivosť a spoľahlivosť detekcie pohybu. [28; 29]



Obrázok 12 Lom IR žiarenia vo Fresnelovej šošovke

(upravené z: [29])

Správne rozmiestnenie PIR detektorov je závislé od charakteru chráneného priestoru a typu použitého snímača, keďže rôzne modely majú odlišné uhly pokrytia, detekčné systémy aj dosahy. Odporúča sa ich namontovať tak, aby sa predpokladaný pohyb potenciálneho narušiteľa odohrával kolmo na os detektora. Na zabezpečenie úplného pokrytia priestoru sa umiestni vhodný počet PIR snímačov tak, aby sa ich zorné polia navzájom dostatočne prekrývali. Čidlá bývajú montované vo výške približne 2 až 3 metre nad úrovňou podlahy a sú orientované tak, aby sa minimalizovali vplyvy zmeny okolitej teploty spôsobené prievanom, prevádzkou ventilácie alebo klimatizácie. PIR detektory by nemali byť nasmerované priamo na okná, vonkajšie dvere, vykurovacie zariadenia, žiarovky či iné zdroje tepla a svetla, pretože tie by mohli vyvolávať falošné poplachy. Rovnako by sa v detekčnom poli nemali nachádzať pohyblivé zavesené predmety, ako sú napríklad lustre či závesy. V priestoroch s podlahovým vykurovaním sa použitie PIR čidiel neodporúča, pretože tepelné toky z vykurovacieho systému môžu viesť k nespoľahlivej detekcii. [28; 29]

2. Ultrazvukové čidlá

Ultrazvukové (Ultrasonic) ďalej už len ako US čidlá sú konštruované tak, aby do stráženého priestoru vysielali mechanické vlny s konštantným kmitočtom, spravidla v pásme nad hranicou ľudského sluchu. V čidle je neustále generovaný ultrazvuk, ktorý odražaním od okolitých povrchov a objektov vytvára ustálený referenčný vzor prijímaného signálu. Ak sa v priestore objaví pohybujúci sa objekt, dôjde k zmene fázy a doby preletu ultrazvukových vln, čo je výsledkom Dopplerovho javu. Táto odchýlka od referenčnej hodnoty je elektronikou ihneď vyhodnotená ako narušenie stráženého priestoru a je zoslané poplachové hlásenie. Všetka potrebná elektronika na generovanie a spracovanie ultrazvukových impulzov je umiestnená priamo v module čidla. Z napájaného meniča sú

ultrazvukové signály vysielané do priestoru cez špeciálny menič, zatiaľ čo prijímač kontinuálne monitoruje odrazené vlny. V kludovom stave sa prijímaný signál nachádza vo vzťahu so signálom vyslaným bez zmeny, a to je považované za normálny stav. Keď sa v stráženom priestore pohne nejaký objekt, zmení sa fáza prijatého ultrazvuku. Táto zmena je porovnaná s nastavenou hodnotou. Ak je rozdiel väčší, než je bežný šum systému, čidlo vyhodnotí situáciu ako poplach.

Pri inštalácii ultrazvukových čidiel sa vyžaduje, aby bol strážený priestor uzavretý, inak by mohli vlny prúdiť do okolitých miestností a vyhodnocovať sa ako narušenie. Čidlo sa nasmeruje tak, aby pravdepodobný pohyb páchatel'a smeroval priamo na menič alebo od neho, čo zabezpečuje maximálnu citlivosť detekcie. Typický dosah týchto čidiel predstavuje približne desať metrov. V prostrediach, kde sú prítomné predmety pohlcujúce ultrazvukové vlny, napríklad hrubé koberce, peny alebo mastné povrchy, sa musí počítať so zmenou citlivosti čidla, keďže takéto materiály môžu ultrazvukové impulzy čiastočne tlmiť. Týmto spôsobom môže dôjsť ku dvojakej chybe. Snímač môže byť po umiestnení nového absorpčného prvku buď príliš citlivý, alebo naopak nereagovať dostatočne. Podobne môže byť ovplyvnený dosah, ak sa do blízkosti zariadenia umiestnia predmety, ktoré voľne visia a môžu sa pohybovať. Ich prítomnosť vedie k falošným poplachom v dôsledku drobných vibrácií. Viacero ultrazvukových čidiel môže byť v jednom priestore využitých len za podmienky, že ich vysielacie sú synchronizované alebo navzájom odladené na iné kmitočty, aby sa vylúčila vzájomná interferencia. Z dôvodu možnosti vzniku falošných poplachov sa nesmú čidlá umiestňovať nad zdroje tepla, ako sú vykurovacie telesá či prieduchy teplovzdušného vykurovania. Rovnako sa vyhýba umiestneniu v blízkosti zariadení generujúcich široké pásmo hluku či v miestnostiach, kde dochádza k častým zmenám zariadenia interiéru, napríklad v skladoch.

Každé ultrazvukové čidlo má možnosť jemného nastavenia dosahu, ktoré sa vykonáva znížením výkonu ultrazvukového meniča až po dosiahnutie požadovaného pokrytia bez nadmernej citlivosti na rušivé vplyvy. Počas kalibrácie je potrebné zvoliť najnižšiu hodnotu výkonu, pri ktorej je ešte zachované úplné pokrytie stráženého priestoru a zároveň sa minimalizuje riziko planých poplachov. Pri každej zmene v usporiadaní interiéru (napríklad pridaní nábytku, inštalácii nových záclon či iných akustických bariér) musí byť rozsah a citlivosť čidla opätovne skontrolované a nastavené. Neodmysliteľnou súčasťou údržby je aj overenie funkčnosti ochranného tamper kontaktu krytu, ktorý zabezpečuje detekciu pokusu o neoprávnené otvorenie puzdra čidla.

3. Mikrovlnné senzory

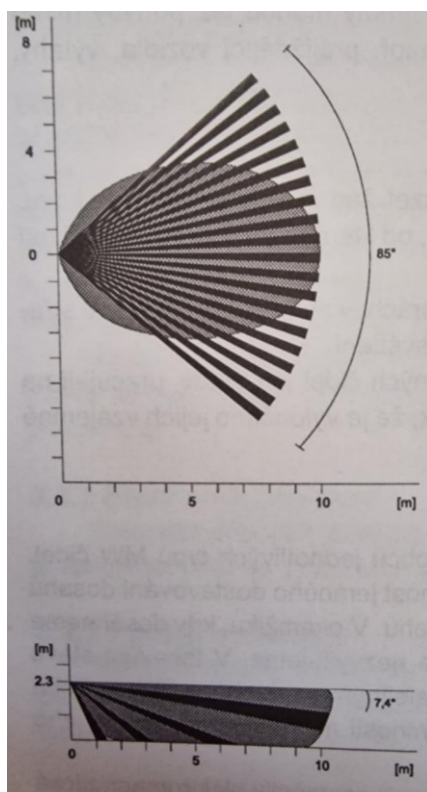
Mikrovlnné (Microwave) ďalej už len ako MW vychádzajú z rovnakého fyzikálneho princípu ako ultrazvukové, no namiesto mechanických vĺn pracujú v oblasti elektromagnetického spektra s typickými kmitočtami okolo 2,5 GHz, 10 GHz alebo 24 GHz. V ich vnútornom zapojení sa nachádza mikrovlnný menič, ktorý vysiela elektromagnetické signály do stráženého priestoru a prijíma ich odrazené späť od okolitých prekážok. V kľudovom stave sú odrazené signály v stabilnom pomere, a preto sa pri absencii pohybu zachytáva prakticky rovnaká odchýlka, ktorá je použitá ako referenčná hodnota. Akonáhle sa v sledovanom priestore pohne objekt, zmení sa fáza alebo amplitúda odrazených vĺn, čo je systémom elektronicky vyhodnotené ako narušenie. Pri inštalácii mikrovlnných čidiel sa kladie dôraz na správnu orientáciu tak, aby pohyb potenciálneho narušiteľa viedol kolmo k osi čidla, teda aby bol umožnený najcitlivejší príjem narušenia. Na dosiahnutie optimálneho pokrytia sa poloha a uhol čidla nastavujú tak, aby jeho dosah zodpovedal charakteru stráženého priestoru, pričom sa sleduje, aby sa mikrovlnné lúče neodrážali od kovových predmetov blízko čidla, čo by mohlo narušiť jeho detekčnú charakteristiku. Z hľadiska falošných poplachov sa vyžaduje, aby sa v blízkosti mikrovlnného senzora nevyskytovali veľké kovové objekty, ktoré by odrážali vysielané vlny a vytvárali odrazy. Ďalej sa mikrovlnné čidlá nesmú osádzať v priestoroch, kde sa môžu počas stráženia spínať svietidlá s kmitočtovým spektrom ako napríklad niektoré typy žiaroviek, pretože by mohlo dôjsť k vyhodnoteniu týchto zmien ako príchodu narušiteľa. V jednej miestnosti sa môže používať viacero mikrovlnných čidiel len za podmienky, že pracujú na odlišných vysielacích frekvenciách alebo sú navzájom pod takým nastavením, že vzájomné rušenie je vylúčené. V interiéroch s častou obmenou usporiadania, napríklad v skladoch, sa použitie mikrovlnných čidiel neodporúča, pretože zmena rozmiestnenia regálov či obložení stien môže viesť k nekorektnej funkcii.

S nastavením dosahu mikrovlnných čidiel sa začína od najnižšej hodnoty, ktorá zodpovedá minimálnemu potrebnému pokrytiu priestoru, a výkon meniča sa postupne zvyšuje len dovtedy, kým sa nedosiahne požadovaná detekčná zóna. Keď je priestor optimálne pokrytý a zároveň je dosah čidla minimálne citlivý na nežiaduce rušenie, nastavovanie sa ukončí. Takto sa zabezpečí, že čidlo pracuje spoľahlivo pri čo najnižšej náchylnosti na falošné poplchy. V rámci pravidelnej údržby sa potom kontroluje, či nedošlo k zmene elektromagnetických podmienok v priestore, v ktorom je čidlo umiestnené, napríklad pridaním kovových predmetov. Akákoľvek zmena v zariadení či prostredí môže

ovplyvniť odraz mikrovln a preto je po každej väčšej úprave okolitého prostredia nutné dosah a citlivosť čidla opätovne skontrolovať a podľa potreby upraviť. Neoddeliteľnou súčasťou tejto kontroly je aj overenie funkcie tamper kontaktu krytu, ktorý pri neoprávnenej manipulácii so snímačom vyvolá alarm. [28; 29]

4. Kombinované (duálne) senzory

Kombinované čidlá, ktoré v sebe spájajú PIR a US princíp, sú navrhované tak, aby sa predišlo falošným poplachom spôsobeným nepriaznivými podmienkami v prostredí. V týchto zariadeniach sa v podstate predpokladá, že je zanedbateľná pravdepodobnosť výskytu dvoch narušení, ktoré by mohli spustiť poplach u jednotlivých systémov fungujúcich na rozdielnych fyzikálnych princípoch. V praxi je kombinácia PIR a US senzora usporiadaná tak, že k vyhláseniu poplachu dôjde len vtedy, keď obidva moduly súčasne zaznamenajú prítomnosť pohybujúceho sa objektu.



Obrázok 13 Charakteristika kombinovaného čidla

(zdroj: [28])

Na predchádzajúcom obrázku je znázornená typická detekčná charakteristika takéhoto kombinovaného čidla. V strede je zobrazený PIR modul, ktorého optický systém je

rozdelený do viacerých úzkych pruhov pokrývajúcich horizontálny uhol približne 85° . Každý pruh je vyčlenený na snímanie infračerveného žiarenia z určitej časti priestoru. V tom istom čase je ultrazvuková sekcia čidla spustená tak, že vytvára jednofarebné oblasti detekcie (tieňovanú tmavšie), ktorá pokrýva približne 10 metrov do priestoru pred čidlom a zaberá úzky uhol asi $7,4^\circ$ vo vertikálnom pláne. Pri bežnom nasadení je v kludovom stave sledované, že v PIR časti nedochádza k zaznamenaniu tepelnej zmeny v žiadnom z vyhradených pruhov, a súčasne ultrazvukový prijímač nerozoznáva zmenu fázového alebo amplitúdového profilu vysielaných vln. Ihneď, keď sa však v niektorej z úzkych infračervených zón objaví pohyb teplej série, napríklad pohybujúca sa osoba, PIR modul vyšle signál do vyhodnocovacej elektroniky. Paralelne k tomu, ak sa v priestore nachádza aj US odraz, sa zaznamená zmena v profile ultrazvukového vlnivého poľa. Keď obidva princípy naraz potvrdia pohyb, čo znamená že PIR vyhodnotí narušenie tepelnej stopy a US potvrdí posun fázy ultrazvuku, je detekcia vyhlásená ako definitívna a poplach sa spustí. Takto je zrejmé, že priestorový pás PIR pokrýva široký uhol 85° , no ultrazvuková zóna je vložená do tohto pruhu ako úzky definovaný lúč v smere šípky v spodnom diagrame, čo zabráňuje zachyteniu pohybu menších zdrojov ako sú malé domáce zvieratá. [28; 29]

3.1.3 Prvky predmetovej ochrany

Pri predmetovej ochrane sú využívané rôzne snímače, ktoré pôvodne boli navrhnuté pre iné účely – napríklad magnetické kontakty, záclonové PIR snímače, mikrovlnné detektory, infračervené závory či reflexné optoelektronické snímače. Na špeciálne zabezpečenie trezorových skríň a komorových trezorov boli vyvinuté tzv. seizmické snímače. V minulosti boli používané aj kapacitné detektory, avšak od nich sa upúšťa pre náročnú montáž, zložité nastavovanie a vyššiu náchylnosť k falošným poplachom. Samostatnú skupinu tvoria závesové a polohové snímače určené na ochranu umeleckých diel.

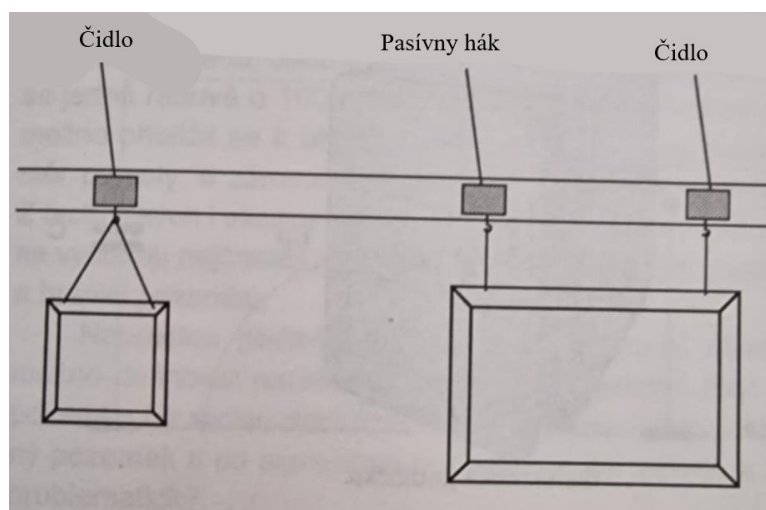
1. Detektory otrasov

Seizmické snímače sú konštruované na princípe selektívneho spracovania vlnenia šíriaceho sa pevnými telesami pri mechanickom alebo tepelnom spracovaní. Pri ich činnosti je u najnovších typov využívané digitálne spracovanie signálu. S týmito zariadeniami je možné monitorovať objekty z materiálov, akými sú kov, betón alebo kameň, zatiaľ čo materiály ako sklo, drevo, guma či penové hmoty nemôžu byť otrasovými snímačmi spoľahlivo chránené. Seizmické snímače sú navrhnuté tak, aby boli schopné reagovať na všetky súčasné spôsoby napadnutia trezorov, peňažných automatov

alebo ťažkých trezorových miestností. K spoľahlivej funkcii seizmických snímačov je nevyhnutné, aby boli namontované na rovný povrch stráženého objektu, pričom musí byť pred montážou odstránená akákoľvek vrstva materiálu tlmiaceho zvuk. Pripojenie k EZS musí umožňovať individuálnu identifikáciu každého snímača, čo sa dosahuje priradením do samostatnej slučky. Pri inštalácii seizmických snímačov sa vychádza z nutnosti zohľadniť vonkajšie vplyvy ktoré by mohli ovplyvniť ich činnosť, napríklad blízke cesty, železničné trate či metro. Plochy prístupné z vonkajšieho nestráženého priestoru by nemali byť chránené seizmickými snímačmi, aby sa zabránilo spusteniu falošného poplachu. Rovnako sa pri montáži predchádza vlhkosti, ktorá by sa mohla dostať do čidla a narušiť jeho funkciu. [28; 29]

2. Snímače na ochranu umeleckých predmetov

Sledovanie umeleckých predmetov sa realizuje pomocou závesových a polohových seizmických čidiel, ktoré zostávajú aktívne aj počas prevádzky výstavných priestorov pre verejnosť. Závesové čidlá sú upevnené na háku nad predmetom pomocou pevného lanka. Piezoelektrický menič zachytáva aj tie najmenšie otrasy prenášané k háku, signál sa zosilní, vyfiltruje a spustí poplachové relé. Citlivosť sa nastavuje tak, aby zodpovedala hmotnosti obrazu či reliéfu čo je zvyčajne od 1 do 100 kilogramu. [28; 29]



Obrázok 14 Aplikácia závesových čidiel

(upravené z: [28])

Pre spoľahlivú činnosť je nevyhnutné pripevniť čidlo na rovný, pevný povrch očistený od vrstiev tlmiacich vibrácie a pripojiť ho do samostatnej poplachovej slučky, aby bola zabezpečená individuálna identifikácia. Polohové čidlá fungujú na princípe

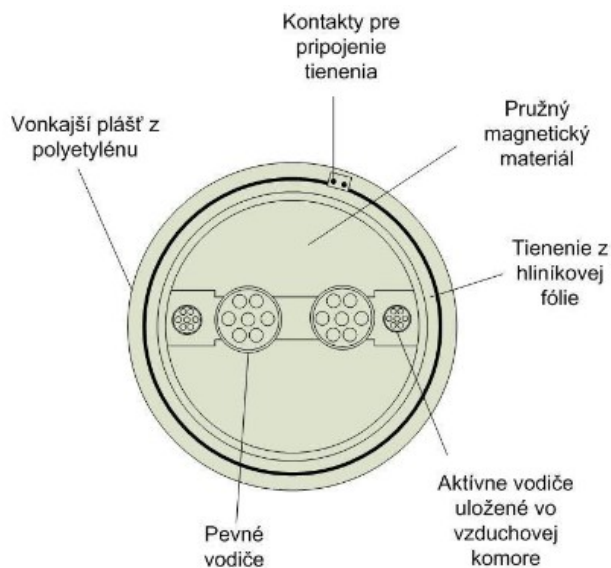
elektromagnetického alebo kontaktového ramienka dotýkajúceho sa povrchu diela. Ak sa ramienko odkloní mimo stanovený uhol alebo sa odtrhne, aktivuje sa magnetický kontakt a spustí poplach. Tento typ sa používa v prípadoch, keď nie je možné zavesiť predmet na lanko. Pri inštalácii oboch riešení je dôležité vyhnúť sa rušivým vplyvom ako napríklad silným vibráciám z blízkej premávky, priemyselným zariadeniam či vetru. Povrchy prístupné z vonkajšieho nestráženého priestoru by sa seizmickými snímačmi nemali chrániť a v miestnostiach s vysokou vlhkosťou je nutné zabezpečiť ochranu čidiel pred kondenzáciou. Pre zabezpečenie spoľahlivej funkcie sa každé čidlo spúšťa a testuje pomocou interného generátora a testovacieho meniča. Citlivosť sa nastavuje na najnižšiu hodnotu, ktorá ešte deteguje pokus o sňatie bez spustenia pri náhodných otrasoch, napríklad pri pohybe návštevníkov. Po každej zmene usporiadania steny či rámu je nutné citlivosť skontrolovať a v prípade potreby upraviť. [28; 29]

3.1.4 Prvky perimetrickej ochrany

Perimetrické senzory sú inštalované na hraniciach rozľahlých areálov, priemyselných podnikov a samostatne stojacich objektov, aby bolo detekované narušenie vonkajšej línie už pri pokuse o vstup. Výber konkrétneho typu senzora je podmienený charakterom terénu, významom chráneného priestoru a požadovanou úrovňou zabezpečenia. Krytie a mechanická konštrukcia vonkajších zariadení sú navrhované tak, aby odolali nepriaznivým poveternostným vplyvom, čo odlišuje tieto komponenty od detektorov, ktoré sú umiestňované vo vnútornom prostredí. Účinnosť perimetrickej ochrany je závislá od existencie pevnej mechanickej bariéry, najčastejšie plotu, bez ktorej by právne postihnutie narušiteľa bolo komplikované. Pri návrhu systému má byť zohľadnené, že senzory nemajú reagovať na bežné vonkajšie javy, akými sú pohyb trávy, listov či konárov, vibrácie plotu vo vetre, prúdenie vzduchu, zrážky, pohyb zvierat alebo doprava v blízkosti hranice pozemku. [28; 29]

1. Mikrofonické káble

Mikrofonický kábel je navrhnutý tak, aby mechanické namáhanie či otrasy snímali a prevádzal ich na elektrický signál, ktorý je následne spracovávaný v analyzačnej jednotke. Zároveň je snímač schopný zaznamenávať aj okolité zvuky, čo umožňuje rozlíšiť charakter prípadného narušenia. Elektrické zapojenie mikrofonických káblov sa líši podľa konkrétneho typu, avšak vo výbave býva vždy zahrnutá ochrana proti preťaženiu či prepätiu, aby sa zabránilo poškodeniu pri pokuse o sabotáž. [28; 29]



Obrázok 15 Konštrukcia mikrofónického kábla

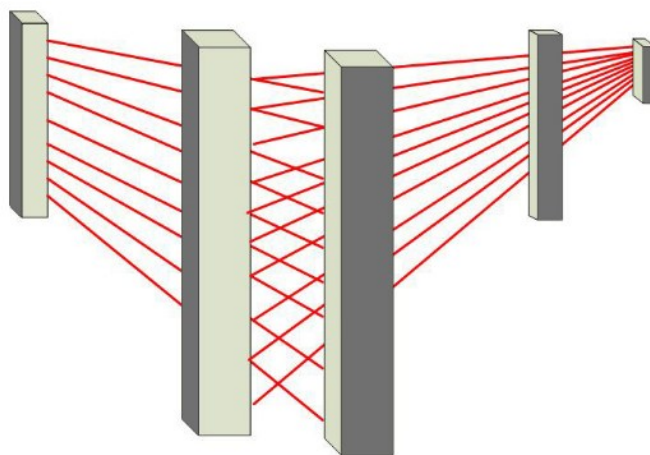
(zdroj: [29])

Mikrofónické káble sa najčastejšie inštalujú priamo do drôtených plotov pri ich výstavbe, pričom existujú modifikované verzie, v ktorých je kábel predom zabudovaný do žiletkovej siete alebo do špeciálnych obranných oplození využívaných napríklad v prístavoch. V prípadoch, keď býva kábel zabetónovaný, schovaný pod omietku alebo zakopaný v zemi, sú náklady na inštaláciu vyššie než pri klasickom upevnení do plota. Jeden úsek snímača môže pokryť vzdialenosť až 300 metrov. Pri prevádzke mikrofónických káblov sa však kladie dôraz na vylúčenie zdrojov falošných poplachov. Medzi rizikové faktory patrí prítomnosť zveri a domácich zvierat, krupobitie, otrasy spôsobené bleskom počas búrky, ale aj silný vietor. Okrem toho môže byť funkcia zariadenia narušená veľmi silným elektrickým či elektromagnetickým pulzom, vyvolaným napríklad priamym úderom blesku. Všetky tieto vplyvy sa pri návrhu a implementácii systému zohľadňujú tak, aby bol dosiahnutý spoľahlivý chod naprieč celým stráženým úsekom. [28; 29]

2. Infračervené závery a bariéry

Infračervené zábrany a bariéry sú vysoko rozšíreným typom vonkajších perimetrických čidiel. Ich princíp spočíva v tom, že medzi vysielačom a prijímačom infračervených lúčov je vytvorené jedno alebo niekoľko synchronizovaných pásiem infračerveného žiarenia. Keď dôjde k prerušeniu niektorého z týchto lúčov, vyhodnotenie na prijímacej strane aktivuje poplach. Aby bol systém odolný voči vonkajším svetelným rušeniam, infrazábrany pracujú v pulznom režime. Kryty vysielačích a prijímacích modulov sú opatrené

vyhrievaním, ktoré zabraňuje oroseniu optiky alebo nánosu vlhkosti z vonkajšej strany. Elektrické zapojenie infračervených bariér sa vždy riadi inštalačným manuálom daného výrobku a zahŕňa štandardnú ochranu proti sabotáži i určené napájacie napätie. Výstup býva vo forme relé, ktoré sa pripája do poplachovej slučky ústredne signalizácie EZS. Inštalácia infrazábrany je náročná na presné osadenie pevných montážnych stanovišť, pretože vysielace aj prijímače musia byť umiestnené na rovnom teréne bez stien, stromov alebo iných prekážok ležiacich v rovine lúčov. Pri viacnásobnom použití modulov na dlhých úsekoch obvodu sa jednotlivé pásma musia čiastočne prekrývať, aby sa zabránilo vzniku miest, kde by detekcia neprerušeného lúča nebola spoľahlivá. [28; 29]



Obrázok 16 Prekrytie infračervených lúčov

(zdroj: [29])

Na obrázku 16 sú viditeľné viaceré stĺpy s prenosovými modulmi, ktoré medzi sebou vytvárajú rad prekrývajúcich sa lúčov. Takáto konfigurácia zabezpečuje, že ak je ktorýkoľvek lúč prerušený, prerušenie je okamžite vyhodnotené ako narušenie perimetra. [28; 29]

3. Mikrovlnné bariéry

Ďalším prvkom vonkajšej perimetrickej ochrany sú mikrovlnné bariéry. Ich princíp spočíva v tom, že medzi vysielacom a prijímačom sa vytvorí elektromagnetické pole v pásme mikrovln č. je zvyčajne okolo 2,5 GHz, 10 GHz alebo 24 GHz. Keď sa do tejto detekčnej zóny dostane pohybujúci sa objekt, napríklad človek, dochádza k zmene parametrov prijímaného signálu, ktorá je okamžite detegovaná a vyhodnotená ako narušenie perimetra. Elektrické pripojenie mikrovlnných bariér je špecifické podľa inštalačného manuálu konkrétneho výrobku a zahŕňa ochranu proti sabotáži i štandardné napájacie

napätie. Výstup je zvyčajne riešený bezpotenciálovým relé, ktoré sa napája do poplachovej slučky ústredne EZS.

Pri montáži mikrovlnnej bariéry je nevyhnutné dodržať diagram čidla tak, aby sa predišlo možným prepadnutiam pod lúčmi čo znamená aby sa žiadna časť perimetra neocitla mimo ochrany. Výška inštalácie nad terénom musí byť taká, aby sa zabránilo podlezeniu osôb pod úrovnou lúču. Medzi rizikové faktory falošných poplachov patria pohyby okolitej vegetácie, no aj náhle zmeny počasia. Mikrovlnný lúč sa nesmie dotýkať drôteného alebo kovového plotu, pretože pohyby oplotenia by mohli spustiť nežiaduce poplchy. V stráženom priestore taktiež nesmú byť pohybujúce sa objekty, ako sú stromy, kríky a podobne.

II PRAKTICKÁ ČASŤ

4 ÚVOD K MERANIAM

V rámci praktickej časti bakalárskej práce boli realizované merania vybraných sieťových kamier značky AXIS, konkrétne modelov M1045-LW, Q1635, P1435-LE, P3225-LVE Mk II a Q3505-V. Merania boli vykonané so zameraním na získanie reálnych údajov o spotrebe elektrickej energie v rôznych prevádzkových režimoch a o objeme dát generovaných pri zázname videa. Tieto údaje sú kľúčové pre vyhodnotenie celkových nákladov na vlastníctvo bezpečnostných kamerových systémov. Každá kamera bola testovaná samostatne v reálnych podmienkach s cieľom simulovať rôzne scenáre jej používania. Merania boli vykonané vo vnútornom priestore laboratória, kde boli kamery nasmerované na statické prostredie s minimálnym pohybom a prepínaním osvetlenia, ako aj nasmerované na vonkajšie prostredie budovy, kde sa počas dňa a noci menili svetelné podmienky, výskyt pohybu a výskyt prachu, čím boli simulované bežné reálne podmienky nasadenia bezpečnostného kamerového systému.

Kamery boli napájané cez PoE switch, konkrétne Mercusys MS110P, ktorý umožňuje napájanie až ôsmich zariadení pomocou ethernetového kábla. Spotreba elektrickej energie bola meraná pomocou meracieho prístroja Solight DT26, pričom bol zaznamenaný odber v rôznych režimoch ako pri bežnej prevádzke bez záznamu a pri aktívnom nahrávaní obrazu. Pred meraním bola hodnota príkonu samotného switchu vopred samostatne odmeraná a následne odpočítaná od celkovej hodnoty, aby bola zabezpečená presnosť výsledkov a aby boli zaznamenané iba skutočné hodnoty spotreby meraného zariadenia. Záznam videa bol ukladajú pomocou softvéru VLC, ktorý umožňuje jednoduché uchovanie dát z IP kamier. Získané videozáznamy boli následne analyzované z hľadiska dátovej náročnosti v závislosti od dĺžky záznamu a snímaného obsahu. Cieľom týchto meraní bolo získať reálne vstupné dáta pre výpočet vybraných položiek celkových nákladov na životnosť kamerových systémov, ako je spotreba energie, veľkosť úložného priestoru a frekvencia záznamu. Takto získané údaje budú ďalej spracované v rámci návrhu výpočtového modelu TCO pre bezpečnostné technológie.

5 MODEL VÝPOČTU CELKOVÝCH NÁKLADOV NA VLASTNÍCTVO (TCO)

Pre účely TCO boli identifikované a rozčlenené jednotlivé nákladové položky, ktoré sa v praxi najčastejšie spájajú s návrhom, implementáciou, prevádzkou a údržbou bezpečnostných systémov typu VSS a PZTS. V nasledujúcom prehľade sú tieto náklady systematicky rozdelené podľa fáz životného cyklu, typu nákladu a ich charakteru. Každá položka je zároveň doplnená stručným opisom jej vplyvu na celkové TCO.

Tabuľka 11 Faktory TCO pre VSS a PZTS podľa fáz životného cyklu a nákladových kategórií

Nákladová položka / Faktor	Fáza Životného Cyklu	Kategória nákladov	Vplyv na TCO
Hardvér			
Cena kamier / senzorov / ústredne / NVR / serverov	B	Priame - CapEx	Základné obstarávacie náklady závisia od typu, kvality a počtu
Kvalita a spoľahlivosť hardvéru	B, D, E, G, I	CapEx, OpEx, Skryté	Vyššia kvalita = vyšší CapEx no nižší OpEx, menej porúch, dlhšia životnosť
Sieťová infraštruktúra (VSS)	B, C	Priame - CapEx	Náklady na switche, routery, kabeláž
Záložné zdroje (akumulátory)	B, E	CapEx, OpEx	Obstarávacía cena a náklady na pravidelnú výmenu
Softvér			
Licencie	B, D, E	CapEx, OpEx	Jednorazové alebo opakované poplatky
Aktualizácie softvéru / firmvéru	E, G	OpEx	Náklady na prácu alebo poplatky za aktualizácie. Kritické pre bezpečnosť a funkčnosť
Inštalácia a implementácia			
Práca technikov	C	Priame - CapEx	Závisí na zložitosti, typu systému, prostredí
Konfigurácia a integrácia	C	Priame - CapEx	Nastavenie systému, prepojenie s inými systémami
Počiatočné školenie	C	Nepriame / CapEx	Náklady na zaškolenie administrátorov a užívateľov
Prevádzka			
Spotreba energie	D	Priame - OpEx	Náklady na elektrinu pro chod komponentov
Úložisko dát	B, D	CapEx, OpEx	Náklady na disky alebo cloudové úložisko
Šírka pásma (VSS - cloud / vzdialený prístup)	D	Priame - OpEx	Náklady na prenos dát
Poplatky za cloud	D, X	Priame - OpEx	Pravidelné poplatky za služby
Personál (monitoring, správa)	D	Priame - OpEx	Mzdové náklady na obsluhu a správu systému

Nákladová položka / Faktor	Fáza Životného Cyklu	Kategória nákladov	Vplyv na TCO
Prevádzka			
Výmena batérií (PZTS - bezdrôtové)	E	Priame - OpEx	Pravidelné náklady na nákup a výmenu batérií
Údržba a opravy			
Plánovaná údržba / revízia	E	Priame - OpEx	Náklady na pravidelné kontroly a údržbu
Neplánované opravy	E	Priame - OpEx / Skryté	Náklady na diagnostiku, prácu technika
Servisné zmluvy	E	Priame - OpEx	Fixné poplatky za servis
Skryté a ostatné náklady			
Prestoje systému	D, E	Skryté	Strata bezpečnosti, produktivity, ušlý zisk
Falošné poplachy	D	Skryté	Čas na verifikáciu, zníženie dôvery
Kybernetická bezpečnosť (VSS)	B, C, D, E	CapEx, OpEx, Skryté	Náklady na prevenciu, detekciu, reakciu a obnovu
Priebežné školenia	D, E	Nepriame - OpEx	Náklady na udržiavanie znalostí personálu
Upgrade a modernizácia	F, G	CapEx, OpEx	Náklady na výmenu zastaralých technológií alebo rozšírenia funkcií
Likvidácia	I	OpEx / Skryté	Náklady na demontáž, recykláciu a zmazanie dát
Príležitostné náklady	Všetky	Skryté	Náklady ušlej príležitosti alternatívnej investície
Kvalita dodávateľa	C, E, F, G	Nepriame / Skryté	Ovplyvňuje kvalitu inštalácie, údržby, podpory a teda aj dlhodobé náklady

(zdroj: vlastný)

Na účely presnejšieho členenia a analýzy nákladov v modeli TCO boli jednotlivé nákladové položky označené A až X, pričom každé písmeno predstavuje konkrétnu kategóriu výdavkov viazaných na určitú fázu životného cyklu riešenia. Táto štruktúra bola prevzatá a prispôbena podľa metodiky spravovanej Národnou architektonickou kanceláriou Českej Republiky, ktorá slúži ako základ pre systematické hodnotenie nákladov na informačné a technologické riešenia vo verejnom sektore. Každá nákladová kategória tak reprezentuje špecifickú oblasť výdavkov v horizonte celého životného cyklu (typicky 5 rokov), pričom sú zohľadnené aj opakované náklady, náklady na údržbu, či inovácie. Použitie tejto metodiky umožňuje komplexný pohľad na celkové náklady vrátane tých, ktoré sa často podceňujú alebo nie sú okamžite viditeľné pri prvotnej investícii.

V nasledujúcej tabuľke sú jednotlivé kódy podrobnejšie vysvetlené s ohľadom na ich obsah, relevantnosť pre výpočet TCO, ako aj ich vzťah k fázam implementácie a prevádzky bezpečnostných technológií.

Tabuľka 12 Kategória nákladov podľa TCO

Kód	Opis nákladovej kategórie
A	Náklady na plánovanie, analýzy, tvorbu zadania a výber riešenia/dodávateľa
B	Obstaranie hardvéru a softvéru (neplatí pre cloudové riešenia)
C	Náklady počas analýzy, vývoja, implementácie, integrácie a skúšobnej prevádzky
D	Prevádzka riešenia a podpora užívateľov (neplatí pre cloud)
E	Údržba systému, opravy a priebežné úpravy (neplatí pre cloud)
F	Realizácia plánovaných projektov na zlepšenie a inovácie systému
G	Realizácia technologických upgradov (modernizácia, rozšírenia)
H	Zvýšené náklady na užívanie riešenia, ak sa vyskytnú
I	Náklady spojené s ukončením, odstavením alebo konzerváciou systému
X	Poplatky za využívanie riešení ako služby (iba pre cloud)
Z	Nepredvídané náklady a nepriraditeľné ku konkrétnej fáze, ktoré ovplyvňujú výber riešenia

(upravené z: [30])

5.1 Zaradenie TCO nákladov podľa fáz životného cyklu

Jednotlivé nákladové položky boli priradené k zodpovedajúcim fázam životného cyklu riešenia v súlade s metodikou TCO publikovanou Ministerstvom vnútra Českej republiky. Každá položka bola posúdená z hľadiska svojho výskytu v čase a dopadu na celkové náklady vlastníctva.

V prípade hardvéru bola cena kamier, senzorov, ústrední, NVR alebo serverov zaradená do fázy obstarania (B), keďže ide o počiatočné investičné výdavky. Kvalita a spoľahlivosť hardvéru bola priradená viacerým fázam (B, D, E, G a I) nakoľko ovplyvňuje nielen životnosť a prevádzkové náklady, ale aj nároky na údržbu, modernizáciu a proces ukončenia systému. Náklady na sieťovú infraštruktúru, ako sú switche, káble a ostatné prvky, boli zaradené do fázy nákupu (B) a fázy integrácie (C), keďže ich inštalácia a konfigurácia sa realizuje v počiatočnom období projektu. Záložné zdroje boli zohľadnené vo fáze nákupu (B) a zároveň vo fáze údržby (E), keďže vyžadujú pravidelnú výmenu.

Licencie softvéru VMS, analytických modulov a firmvérov boli zaradené do fázy obstarania (B), pričom ich využívanie pokračuje počas prevádzky (D) a údržby (E). Náklady na aktualizácie softvéru a firmvéru boli priradené do fázy údržby (E) a zároveň modernizácie (G), keďže ide o kontinuálny proces zvyšovania bezpečnosti a funkčnosti systému.

Činnosti ako inštalácia, konfigurácia, integrácia a počiatočné školenie boli priradené do fázy implementácie (C), pretože prebiehajú v úvode zavádzania systému. Spotreba elektrickej energie bola priradená do fázy prevádzky (D), podobne ako náklady na úložisko

dát ktoré môžu spadať do fázy obstarania (B) pri lokálnom riešení alebo do prevádzky (D) v prípade cloudových úložísk. Šírka pásma potrebná na vzdialený prístup alebo cloud bola priradená k prevádzke (D), rovnako ako poplatky za cloudové služby, služby PCO alebo SIM (Subscriber identity Module) karty, ktoré spadajú do prevádzky (D) a modelu služby (X). Prevádzkové výdavky boli ďalej doplnené o náklady na personál a výmenu batérií v bezdrôtových zariadeniach (E).

Plánovaná údržba, revízie, opravy a servisné zmluvy boli logicky zaradené do fázy údržby (E), pričom aj neplánované opravy predstavujú túto etapu. Skryté a nepriame náklady ako prestoje systému alebo falošné poplchy boli priradené do fáz prevádzky (D) a údržby (E), nakoľko sú dôsledkom prevádzkových a údržbových nedostatkov. Kybernetická bezpečnosť bola identifikovaná ako priebežná požiadavka, ovplyvňujúca celý cyklus od výberu technológie (B), cez jej implementáciu (C), prevádzku (D) až po údržbu a reakciu na incidenty (E). Priebežné školenia boli zaradené do fáz (D a E) ako súčasť udržiavania odbornosti personálu. Modernizácia a technologické zlepšovanie systému boli zaradené do fáz (F a G), keďže predstavujú plánované rozširovanie a upgrade systému. Likvidácia riešenia bola zaradená do záverečnej fázy (I), kde sú zohľadnené náklady na demontáž, recykláciu a správne ukončenie prevádzky. Oportúnne náklady boli priradené naprieč všetkými fázami, keďže predstavujú nepriame výdavky spojené s nevyužitými príležitosťami alebo zmeškanými investíciami. Nakoniec, kvalita dodávateľa alebo integrátora bola zohľadnená v etapách implementácie (C), údržby (E), zlepšovania (F) a modernizácie (G), nakoľko ovplyvňuje kvalitu výstupu a dlhodobé náklady na prevádzku a rozvoj systému.

Týmto spôsobom bolo zabezpečené komplexné rozdelenie nákladov podľa ich výskytu a významnosti v životnom cykle riešenia s cieľom objektívneho stanovenia celkových nákladov vlastníctva.

5.2 Analýza kategórie nákladov

Každá z nákladových položiek uvedených v tabuľke bola priradená k jednej alebo viacerým nákladovým kategóriám na základe svojej ekonomickej a funkčnej povahy. Kategórie CapEx a OpEx vyjadrujú, či sa jedná o investičný alebo prevádzkový výdavok. Rozlíšenie na priame, nepriame alebo skryté náklady vychádzalo z možnosti ich priameho priradenia ku konkrétnemu komponentu alebo z miery, akou sa premietajú do účtovných alebo neúčtovných dopadov.

Cena kamier, senzorov, ústrední, NVR a serverov bola zatriedená medzi priame investičné náklady (CapEx). Toto priradenie vyplýva z toho, že ide o jednorazové náklady na obstaranie základných technických komponentov systému. Ich investičný charakter je daný tým, že zvyšujú hodnotu systému a sú aktivované ako súčasť majetku. Zároveň sa jedná o náklady priame, keďže ich výška je známa vopred, je jednoznačne priradená ku konkrétnym zariadeniam a predstavuje základnú zložku investície.

Kvalita a spoľahlivosť hardvéru bola priradená ku kategóriám CapEx, OpEx a skrytým nákladom. Investičný charakter (CapEx) vyplýva z toho, že zariadenia vyššej kvality bývajú drahšie a ich obstaranie sa vykonáva v rámci vstupnej investície. Zároveň sa predpokladá, že spoľahlivejší hardvér si vyžiada nižšie náklady na opravy a výmeny počas životnosti systému, čím sa znižujú prevádzkové náklady (OpEx). Skryté náklady boli priradené z dôvodu, že nízka kvalita môže viesť k častejším poruchám, prestojom alebo incidentom, ktorých dopad nie je bežne evidovaný, ale reálne ovplyvňuje bezpečnosť a funkčnosť riešenia.

Sieťová infraštruktúra (VSS) bola klasifikovaná ako priamy investičný náklad (CapEx). Obstaranie sieťových prvkov, ako sú switche, routery a kabeláž, je nevyhnutné pre prevádzku systému a realizuje sa jednorazovo v rámci inštalácie. Priradenie ku CapEx bolo odôvodnené tým, že ide o technické vybavenie so strednodobou až dlhodobou životnosťou. Keďže tieto prvky slúžia konkrétnym častiam systému a sú súčasťou jeho technickej architektúry, boli náklady označené ako priame.

Záložné zdroje (akumulátory) boli priradené ku kategóriám CapEx a OpEx. Náklady investičného typu (CapEx) vznikajú pri počiatočnom obstaraní záložných systémov, ktoré zabezpečujú napájanie v prípade výpadku elektrickej siete. Prevádzkové náklady (OpEx) sa spájajú s pravidelnou výmenou akumulátorov počas životnosti systému. Tieto výdavky sú podmienené technickou životnosťou batérií a cyklami údržby.

Licencie na softvér boli priradené k nákladovým kategóriám CapEx a OpEx. V prípadoch, keď sa licencia obstaráva jednorazovo, ide o investičný náklad, keďže sa aktivuje ako súčasť systému a používa sa počas celej jeho životnosti. Ak je licenčný model založený na pravidelných poplatkoch, napríklad ročných alebo mesačných, náklady sa evidujú ako prevádzkové.

Aktualizácie softvéru a firmvéru boli zaradené medzi prevádzkové náklady (OpEx). Dôvodom je ich pravidelný výskyt počas životnosti systému a ich priamy vzťah

k udržiavaniu funkčnosti, bezpečnosti a kompatibility softvérových komponentov. Tieto aktualizácie sú nevyhnutné na ochranu systému pred zraniteľnosťami a ich nákladová povaha zodpovedá bežnej technickej správe.

Práca technikov bola zaradená medzi priame investičné náklady (CapEx). Táto klasifikácia vyplýva z toho, že ide o jednorazový výdavok realizovaný počas inštaláčnej fázy systému, ktorý zahŕňa montážne a kabelážne práce vykonávané na mieste inštalácie. Tieto činnosti sú nevyhnutnou súčasťou fyzického uvedenia systému do prevádzky a ich rozsah býva obvykle špecifikovaný v zmluve. Vzhľadom na to, že sú vykonávané jednorazovo a možno ich priradiť ku konkrétnym komponentom systému, bol náklad klasifikovaný ako priamy a investičný.

Konfigurácia a integrácia bola rovnako priradená k priamym investičným nákladom (CapEx). Tento výdavok zahŕňa činnosti súvisiace s nastavením systémových parametrov, logiky detekcie, správy záznamov či prepojenia s inými bezpečnostnými technológiami. Tieto aktivity sa uskutočňujú v rámci implementácie a ich výsledkom je zabezpečenie plnej funkčnosti systému podľa požiadaviek prevádzkovateľa. Keďže sa konfigurácia týka konkrétnych častí systému a realizuje sa jednorazovo, bola považovaná za náklad priamy a investičný.

Počiatočné školenie bolo v tabuľke klasifikované ako nepriamy investičný náklad (CapEx). V tomto prípade sa jedná o náklady spojené so zaškolením administrátorov a užívateľov systému, ktoré sa vykonávajú počas fázy uvedenia systému do prevádzky. Nepriamosť nákladu spočíva v tom, že nie je priamo viazaný na konkrétnu technickú zložku riešenia, ale na zabezpečenie kompetencií personálu. Napriek tomu, že školenie nemá fyzický výstup, jeho realizácia je nevyhnutná pre efektívne a bezpečné používanie systému. Z toho dôvodu bol zachovaný investičný charakter nákladu.

Spotreba energie bola zaradená medzi priame prevádzkové náklady (OpEx). Ide o výdavok, ktorý vzniká počas každodennej činnosti systému a je priamo závislý od počtu, typu a prevádzkovej doby jednotlivých komponentov, ako sú kamery, ústredne, záznamové zariadenia alebo sieťové prvky. Spotreba elektrickej energie je štandardne merateľná a jej nákladová zložka je evidovaná priebežne počas celej životnosti systému. Vzhľadom na možnosť jednoznačne určiť podiel spotreby konkrétnych častí riešenia sa tento náklad považoval za priamy.

Úložisko dát bolo klasifikované ako kombinácia investičného (CapEx) a prevádzkového nákladu (OpEx). Ak sú záznamy ukladané na vlastné diskové polia alebo servery, ide o jednorazovú investíciu do fyzického úložného priestoru, ktorá je účtovaná ako kapitálový výdavok. V prípade využívania cloudového úložiska vznikajú pravidelné platby za služby, ktoré sú evidované ako OpEx.

Šírka pásma pri vzdialenom prístupe alebo cloudovom prenose dát bola priradená medzi priame prevádzkové náklady (OpEx). Náklady tohto typu vznikajú pri prenose video streamu, notifikácií alebo pri synchronizácii dát so vzdialenými úložiskami. Ich výška je závislá od objemu prenesených dát a frekvencie prenosu. Vzhľadom na to, že sú spojené s konkrétnou funkcionalitou systému, napríklad prístup cez mobilnú aplikáciu, ide o náklady priamo súvisiace s jeho každodennou prevádzkou.

Poplatky za cloud boli rovnako zatriedené medzi priame prevádzkové náklady (OpEx). Tieto výdavky predstavujú pravidelne účtované poplatky za cloudové služby, či už ide o ukladanie dát, analytiku, spracovanie záznamov alebo integráciu do systémov tretích strán. Ich pravidelnosť a priama väzba na objem spracovávaných informácií v systéme VSS určuje, že ide o výdavok priamy a zároveň prevádzkový.

Personál vykonávajúci monitoring a správu systému bol zahrnutý medzi priame prevádzkové náklady (OpEx). V tomto prípade ide najmä o mzdy pracovníkov dohľadových centier, technikov správy systému či iných prevádzkových rolí. Ich náklady vznikajú priebežne počas celej životnosti systému a sú úzko spojené s jeho činnosťou. Keďže tieto osoby pracujú výlučne so systémom a zabezpečujú jeho funkciu, sú tieto náklady priradené priamo.

Výmena batérií v bezdrôtových zariadeniach, ako sú detektory alebo sirény v PZTS, bola klasifikovaná ako priamy prevádzkový náklad (OpEx). Vzhľadom na obmedzenú životnosť batérií a potrebu ich pravidelnej výmeny ide o predvídateľný a opakovane sa vyskytujúci výdavok. Tento náklad je ľahko priraditeľný ku konkrétnym zariadeniam a komponentom systému, čo odôvodňuje jeho zaradenie medzi priame náklady.

Plánovaná údržba a revízie boli zatriedené medzi priame prevádzkové náklady (OpEx). Tieto výdavky zahŕňajú pravidelné kontroly technického stavu systému, testovanie funkčnosti komponentov a vykonávanie zákonom alebo normami stanovených revízných úkonov. Keďže sa tieto zásahy uskutočňujú opakovane počas prevádzky systému a vzťahujú

sa na konkrétne zariadenia alebo subsystémy, ich výdavky zodpovedajú bežnému prevádzkovému nákladu a zároveň ich možno priamo priradiť ku konkrétnej zložke systému.

Neplánované opravy boli klasifikované ako priame prevádzkové náklady (OpEx), pričom v niektorých prípadoch aj ako skryté náklady. V prípade štandardných porúch a zásahov, ktoré si vyžadujú diagnostiku alebo výmenu komponentov, ide o priamo identifikovateľné prevádzkové výdavky, ktoré sa vzťahujú na konkrétne technické prvky. Skrytý charakter nákladu nastáva vtedy, keď neplánovaná porucha spôsobí prestoj systému, zníženie bezpečnosti alebo vyžaduje urgentný servisný výjazd, ktorého ekonomický dopad nie je vopred predvídateľný ani evidovaný v rozpočtovej dokumentácii, no ovplyvňuje celkové náklady na vlastníctvo.

Servisné zmluvy boli zaradené medzi priame prevádzkové náklady (OpEx). Ide o zmluvne dohodnuté výdavky na zabezpečenie technickej podpory, údržby, pravidelných kontrol a pohotovostných zásahov. Tieto náklady majú fixný alebo periodický charakter a ich výška je stanovená na základe rozsahu poskytovaných služieb a počtu krytých komponentov. Vzhľadom na ich jednoznačnú viazanosť ku konkrétnemu systému alebo jeho častiam boli tieto náklady označené ako priame.

Prestoje systému boli klasifikované ako skryté náklady. Tento typ výdavku vzniká v prípadoch, keď je systém či jeho časť dočasne nefunkčná v dôsledku poruchy, údržby, výpadku konektivity alebo iného prevádzkového narušenia. Takýto prestoj síce nepredstavuje priamy účtovateľný výdavok, no jeho dôsledky môžu viesť k strate bezpečnosti, obmedzeniu prevádzky alebo zníženiu dôvery užívateľa v spoľahlivosť systému. Keďže tieto dopady nie sú spravidla zachytávané v nákladových prehľadoch, ide o náklady, ktoré sa označujú ako skryté.

Falošné poplachy boli takisto zatriedené medzi skryté náklady, nakoľko vedú k vynakladaniu času na ich verifikáciu, znižujú dôveryhodnosť systému a môžu spôsobovať zbytočné výjazdy zásahových jednotiek. Tieto náklady sú mimoriadne ťažko merateľné a často nie sú zahrnuté v prevádzkových rozpočtoch, no majú dlhodobý negatívny vplyv na efektívnosť a spoľahlivosť zabezpečovacích systémov.

Kybernetická bezpečnosť systému VSS bola klasifikovaná ako kombinácia investičných (CapEx), prevádzkových (OpEx) a skrytých nákladov. Do CapEx boli zahrnuté náklady na obstaranie bezpečnostných prvkov, ako sú šifrovacie nástroje, bezpečnostné moduly alebo sieťové firewally. Prevádzkový charakter bol identifikovaný pri nákladoch

na ich aktualizáciu, správu, testovanie a audit. Skryté náklady boli priradené z dôvodu, že incidenty v oblasti kybernetickej bezpečnosti môžu mať dopad na stratu údajov, kompromitáciu systému alebo zneužitie údajov, čo sa v mnohých prípadoch neodráža priamo v nákladových položkách, ale spôsobuje reálne finančné škody.

Priebežné školenia boli zaradené medzi nepriame prevádzkové náklady (OpEx). Tieto výdavky slúžia na priebežné udržiavanie znalostí a kompetencií personálu. Keďže nie sú viazané na konkrétny komponent a majú charakter podpornej činnosti, ktorá ovplyvňuje efektivitu a bezpečnosť systému ako celku, ide o náklady nepriame. Ich opakovanosť a spojenie s prevádzkou systému zároveň určujú ich zaradenie do prevádzkových výdavkov.

Upgrade a modernizácia boli priradené ku kategóriám CapEx a OpEx. Investičné náklady vznikajú v prípade, že je nutné zakúpiť nové zariadenia, servery alebo softvérové moduly s rozšírenou funkčnosťou. Prevádzková časť sa spája s výdavkami na rekonfiguráciu, migráciu dát, inštaláciu a testovanie. Táto položka predstavuje prirodzený výdavok počas dlhšej životnosti systému, keď je potrebné reagovať na technologický vývoj alebo legislatívne zmeny.

Likvidácia systému bola klasifikovaná ako kombinácia prevádzkových (OpEx) a skrytých nákladov. Do prevádzkových nákladov boli zaradené výdavky spojené s demontážou zariadení, recykláciou hardvéru alebo zmazaním dát z úložísk. Skryté náklady môžu vzniknúť v prípade, že sú porušené legislatívne povinnosti pri likvidácii citlivých údajov.

Príležitostné náklady boli zaradené medzi skryté náklady, nakoľko vyjadrujú hodnotu ušlých príležitostí, ktoré vznikli v dôsledku nevhodného rozhodnutia, omeškania investície alebo nevyužitia dostupných možností. Ide o náklady, ktoré sa spravidla nevyčísľujú v účtovníctve, no ich dopad môže byť značný, najmä v porovnaní s alternatívnymi riešeniami s vyššou efektivitou či návratnosťou.

Kvalita dodávateľa bola zatriedená ako kombinácia nepriamych a skrytých nákladov. Nepriamosť tejto položky spočíva v tom, že nekvalitná dodávka, nedostatočné zaškolenie, slabá dokumentácia alebo chýbajúca podpora nevedú priamo k zvýšeniu nákladov na konkrétny komponent, ale zvyšujú záťaž na správu systému ako celku. Zároveň môže nekvalitný dodávateľ spôsobiť chyby pri implementácii alebo oneskorenie, ktorých dôsledky sa prejavujú skrytým spôsobom, či už v podobe prestojov, reklamácií alebo ďalších škôd.

5.3 Matematický model TCO a praktický evaluačný algoritmus

Pre praktické posúdenie TCO v bezpečnostných technológiách bol zostavený matematický model. Tento model sa opiera o namerané dáta a odhady použité v praktickej časti tejto práce. Zameriava sa na výpočet TCO pre testované VSS a PZTS.

5.3.1 Základné zložky modelu TCO:

1. kapitálové výdavky (CapEx) – predstavujú hlavné náklady na obstaranie hardvéru kamier, ako sú uvedené v Tabuľke 19. Pre systém PZTS by bolo potrebné tieto náklady odhadnúť externe;
2. prevádzkové výdavky (OpEx) – sú opakujúce sa náklady počas 5 ročnej životnosti systému.

$$OpEx_{Celkovo} = OpEx_{ročne} * 5 [roky]$$

Ročné prevádzkové náklady zahŕňajú :

- náklady na energiu vypočítané z priemernej spotreby z Tabuľky 13 pre kamery, Tabuľky 20 pre PZTS a ceny elektriny 0,20 €/kWh;

$$C_{EnergiaRočne} [€] = \left(\frac{P_{Priemer} [W] * 24 [hodín] * 365 [dní]}{1000} \right) * 0,20 [€/kWh] ;$$

kde sa číslom 1000 delí pre premenu W na kWh;

- náklady na cloudové úložisko vypočítané z hodinovej dátovej náročnosti kamier z Tabuľky 14 a ceny 100 €/TB/rok;

$$Ročná\ potreba\ [TB] = \frac{Objem_{dát_{hod}} \left[\frac{MB}{h} \right] * 24 [hodín] * 365 [dní]}{1024^2} ;$$

kde sa číslom 1024^2 delí pre premenu z GB na TB;

$$C_{ÚložiskoRočne} [€] = Ročná\ potreba\ [TB] * 100 \left[\frac{€}{\frac{TB}{rok}} \right] ;$$

- náklady na údržbu a servis kamier odhadnutých na 60 € alebo 80 € ročne. Pre PZTS by tieto náklady bolo potrebné doplniť externým odhadom. Pre úplné OpEx by sa sem rátali priebežné licencie, personál a konektivita ktoré neboli predmetom meraní.

5.3.2 Celkové náklady na vlastníctvo v tomto modeli:

Pre každý komponent sa TCO vypočíta ako :

$$TCO[€] = CapEx [€] + ((C_{Energia_{Ročne}} [€] + C_{Úložisko_{ročne}} [€] + C_{Údržba_{Ročne}} [€]) * 5[roky])$$

kde sú výpočty pre testované kamery uvedené v Tabuľke 19.

5.3.3 Modelovanie TCO pre rôzne scenáre

Model umožňuje vypočítať TCO pre systémy zložené z testovaných komponentov.

1. Scenár 1 – systém s jednou konkrétnou testovanou kamerou

TCO sa prevezme priamo z výpočtov v Tabuľke 19.

$$TCO_{M1045LW} = 8\,765,05\,€$$

2. Scenár 2 – integrovaný systém

$$TCO_{P1435LE} = 14\,701\,€$$

$$TCO_{PZTS}[€] = CapEx_{PZTS}[€] + ((C_{Energia\,PZTS_{Ročne}}[€] + C_{Údržba\,PZTS_{Ročne}}[€]) * 5)$$

$$CapEx_{PZTS} = Odhadom\,300\,€$$

$$OpEx_{PZTS_{Ročne}}[€] = C_{Energia\,PZTS_{Ročne}}[€] + C_{Údržba\,PZTS_{Ročne}}[€]$$

$$TCO_{PZTS} = 300\,€ + ((10,22\,€ + (odhadom)25\,€) * 5) = 476,1\,€$$

$$TCO_{Systém}[€] = TCO_{Kamera}[€] + TCO_{PZTS}[€]$$

$$TCO_{Systém} = 14701\,€ + 476,1\,€ = 15177,1\,€$$

5.3.4 Praktický evaluačný algoritmus

Nasledujúce kroky slúžia na vyhodnotenie TCO pomocou dát z tejto práce:

1. definícia systému – tu sa určí, ktoré testované kamery a či aj PZTS systém budú súčasťou hodnoteného scenára;
2. zber dát pre komponenty –

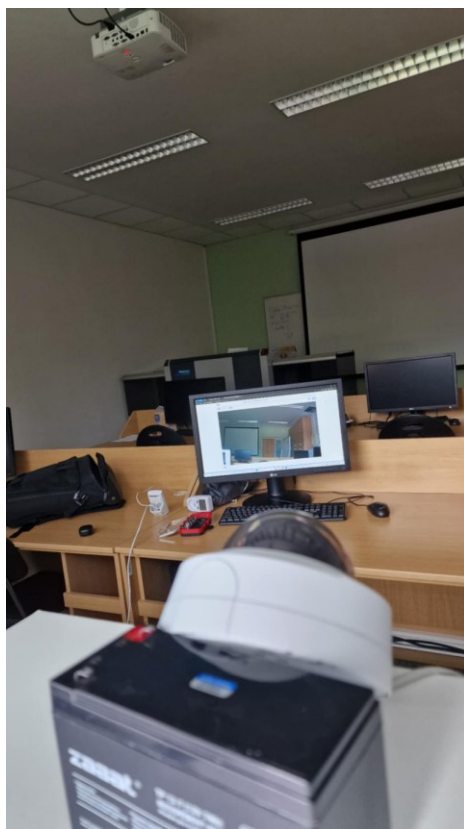
- pre každú vybranú kameru $CapEx$ z Tabuľky 19, $P_{Priemer}[W]$ z Tabuľky 13, $Objem_{Dáta/hodina}[MB/h]$ z Tabuľky 14, $C_{Údržba_{Ročne}}[€]$;
 - pre PZTS $P_{PZTS}[W]$ z Tabuľky 20, externý odhad pre $CapEx_{PZTS}[€]$ a $C_{Údržba_{PZTS_{Ročne}}}[€]$;
 - spoločné $Cena_{kWh}[€]$, $Cena_{TB_{Cloud_{Rok}}}[€]$, $T_{Životnosť}[roky]$;
3. výpočet ročných OpEx pre každý komponent –
- vypočítajú sa $C_{Energia_{Ročne}}[€]$, $C_{Úložisko_{Ročne}}[€]$ (len pre kamery) a použije sa $C_{Údržba_{Ročne}}[€]$;
4. výpočet TCO pre každý komponent –
- $TCO_{Komponent}[€] = CapEx[€] + (OpEx_{Ročne}[€] * 5[roky])$;
5. výpočet TCO pre celý systém kde sa sčíta TCO jednotlivých komponentov;
6. vyhodnotenie kde sa porovnávajú TCO rôznych systémových konfigurácií. Zohľadní sa nielen cena, ale aj miera splnenia bezpečnostných požiadaviek.

6 SCENÁRE A PODMIENKY TESTOVANIA

Merania boli realizované v rôznych prevádzkových scenároch s cieľom zohľadniť vplyv prostredia, osvetlenia a pohybu na energetickú náročnosť a objem generovaných dát dohľadových kamier. Každé zariadenie bolo testované jednotlivo, pričom boli zachované rovnaké technické podmienky a metodika záznamu.

Testovanie bolo uskutočnené v nasledovných prostrediach:

- **vnútorné priestory** – konkrétne v laboratórnom prostredí s minimálnym pohybom, stabilnými svetelnými podmienkami a nízkou dynamikou scény;



Obrázok 17 Kamera smerujúca
na vnútorné priestory laboratória

(zdroj: vlastný)

- **vonkajšie prostredie** – snímanie bolo realizované z vnútra laboratória na okolie budovy pri otvorenom a zatvorenom okne, kde dochádzalo k prirodzeným zmenám osvetlenia (prechody medzi dňom a nocou) a k neustálým pohybom ako napríklad vlnenie stromov a lístia spôsobené vetrom,

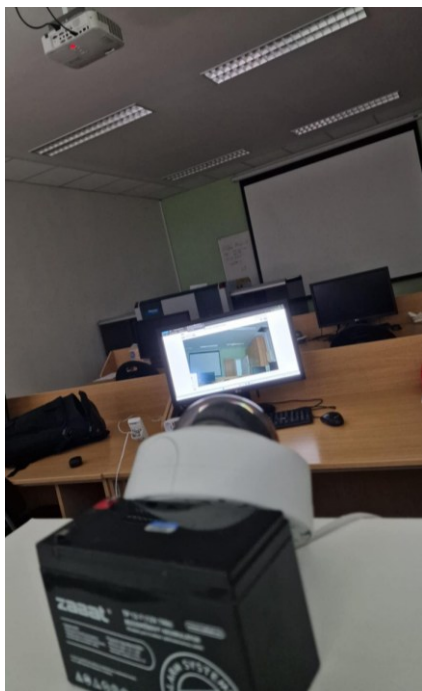
zrážok alebo pohybu osôb. Lokalita zároveň vykazovala vyššiu prašnosť, čo mohlo ovplyvniť snímáciu technológiu a IR osvetlenie;



Obrázok 18 Kamera smerujúca
na vonkajšie prostredie

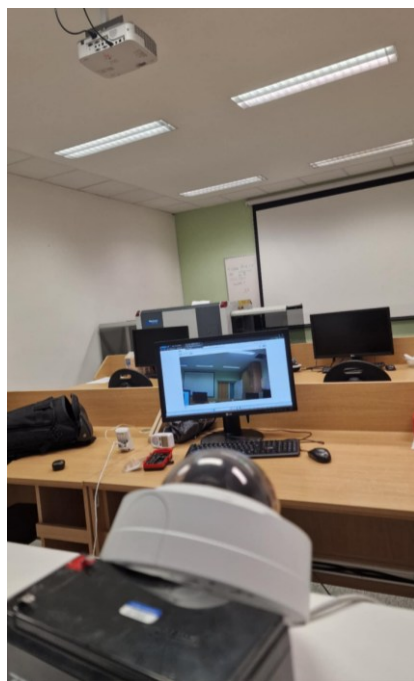
(zdroj: vlastný)

- **prechodové podmienky** – boli zaznamenané aj sekvencie s premenlivými svetelnými podmienkami, ktoré simulovali rýchly prechod medzi svetlom a tmou. Tento prechod bol realizovaný zapínaním a vypínaním osvetlenia v miestnosti, čo umožnilo sledovanie správania kamery pri zapnutí funkcií ako WDR alebo IR prísvit.



Obrázok 19 Kamera snímajúca
prechodové podmienky
(zhasnuté svetlo)

(zdroj: vlastný)



Obrázok 20 Kamera snímajúca
prechodové podmienky
(zapnuté svetlo)

(zdroj: vlastný)

V každom scenári bolo kamerové zariadenie napájané prostredníctvom PoE pomocou switchu Mercusys MS110P a videozáznam bol zaznamenávaný softvérom VLC Media Player. Pre každý typ prostredia bol zaznamenaný výsledný objem dát a bola zaznamenaná aj spotreba elektrickej energie počas aktívneho nahrávania. Tieto podmienky boli zvolené s cieľom čo najvernejšie nasimulovať skutočné prevádzkové scenáre a získať reálne údaje pre následné spracovanie v rámci výpočtu TCO.

7 MERANIE SPOTREBY ELEKTRICKEJ ENERGIE

Spotreba elektrickej energie bola sledovaná pri každom testovanom kamerovom modeli s cieľom získať reálne vstupy pre prevádzkovú časť výpočtu TCO. Merania boli vykonané jednotnou metodikou.

7.1 Postup merania

Každá testovaná kamera bola pripojená k samostatnému PoE portu osemportového switchu Mercusys MS110P. Medzi napájací adaptér switchu a elektrickú sieť bol zapojený zásuvkový merač spotreby Solight DT26, pomocou ktorého bola priebežne sledovaná spotreba elektrickej energie. Ako referenčná hodnota bola najprv zaznamenaná spotreba samotného switchu bez pripojenej záťaže, ktorá bola následne odpočítaná od všetkých ďalších meraní. Na obrázku 21 je znázornené zapojenie merača spotreby elektrickej energie, ktorý je pripojený do elektrickej siete. Do merača je následne pripojený sieťový switch, prostredníctvom ktorého je zabezpečené sieťové prepojenie jednotlivých zariadení. Zo switchu sú vedené tri ethernetové káble. Jeden z nich je pripojený priamo ku kamere, druhý slúži na pripojenie switchu k internetu a tretím je zabezpečené pripojenie počítača k internetu cez switch.



Obrázok 21 Zapojenie merača, switchu a kamery

(zdroj: vlastný)

Každá kamera bola meraná zvlášť a postupne v dvoch režimoch a to nečinnosť a záznam. V každom režime bolo meranie realizované počas intervalu jednej hodiny. Počas tejto doby boli manuálne zaznamenané všetky zmeny príkonu zobrazené na displeji wattmetra. Zaznamenané boli minimálne a maximálne hodnoty príkonu, ktoré sa objavili v priebehu merania, pričom minimálna hodnota zodpovedala najnižšiemu pozorovanému príkonu a maximálna hodnota reprezentovala najvyšší zaťažovaný stav.

7.2 Spracovanie údajov

Hodnota priemerného príkonu bola následne vypočítaná ako priemer medzi minimálnou a maximálnou hodnotou podľa rovnice:

$$P_{Priemer} [W] = \frac{P_{min} [W] + P_{max} [W]}{2};$$

kde číslo 2 v menovateli vyjadruje počet hodnôt, ktoré sa priemerujú. Takto vypočítaný priemer príkonu bol následne dosadený do výpočtu energie podľa rovnice:

$$E [Wh] = P_{Priemer} [W] * t [hodín];$$

kde čas merania bol jednotný a to, $t = 1$ hodina. Takto získané hodnoty boli zaznamenané v Tabuľke 13 a predstavujú energetický profil každého testovaného kamerového modelu pre jednotlivé režimy prevádzky.

Tabuľka 13 Spotreba elektrickej energie

Kamera	Režim	Minimálny príkon P [W]	Maximálny príkon P [W]	Priemerný príkon P [W]	Čas t [h]	Energia E [Wh]
AXIS M1045-LW	nečinnosť	2	2,8	2,5	1	2,5
	záznam	2,6	3,6	3,2	1	3,2
AXIS Q1635	nečinnosť	6,2	7,5	7	1	7
	záznam	8,4	10,5	9,5	1	9,5
AXIS P1435-LE	nečinnosť	5,2	6,5	6	1	6
	záznam	6,6	8,2	7,5	1	7,5
AXIS P3225-LVE Mk II	nečinnosť	4,2	5,8	5	1	5
	záznam	5,5	7,2	6,2	1	6,2
AXIS Q3505-V	nečinnosť	4,8	6,1	5,5	1	5,5
	záznam	6,3	8,1	7	1	7

(zdroj: vlastný)

Takto získané údaje budú priradené ku každému mu kamerovému modelu a budú využité pri zostavovaní päťročného prevádzkového rozpočtu v kapitole o výpočte TCO.

8 MERANIE DÁTOVEJ NÁROČNOSTI VIDEOZÁZNAMU

Pozornosť bola venovaná analýze dátovej náročnosti videozáznamov, ktoré sú produkované modernými IP kamerami v rôznych prevádzkových podmienkach. Táto časť meraní predstavuje dôležitý vstup do hodnotenia TCO, keďže ovplyvňuje požiadavky na úložisko, šírku prenosového pásma, ako aj prevádzkové náklady súvisiace s prenájmom cloudových služieb alebo obstaraním sieťovej infraštruktúry.

8.1 Cieľ merania a metodika

Za cieľ bolo stanovené merať dátovú náročnosť videozáznamov produkovaných vybranými modelmi IP kamier v rôznych typoch sledovaných scén. Meranie bolo vykonané s cieľom získať realistické vstupné údaje pre výpočet požiadaviek na úložisko a prenosovú infraštruktúru, ktoré tvoria dôležitú súčasť prevádzkových nákladov započítavaných do modelu TCO. Pre každú kameru boli vytvorené tri typové scény a to statický interiér bez pohybu, exteriér s pohybom stromov, listov, premenlivého počasia a napokon interiérová scéna s premenlivými svetelnými podmienkami. Tie boli zabezpečené manuálnym prepínaním osvetlenia v miestnosti počas záznamu, čo spôsobovalo časté zmeny expozície a aktiváciu funkcií ako WDR či IR prísvit. Záznam každej scény bol realizovaný v trvaní jednej hodiny pri rozlíšení Full HD pri 25 snímkach za sekundu a s použitím kompresie v závislosti od možností danej kamery. Po ukončení záznamu bola zaznamenaná veľkosť výstupného súboru v MB.

8.2 Zistenia a priebežné hodnotenie

Zo získaných údajov vyplynulo, že dátová náročnosť sa výrazne líši v závislosti od typu prostredia a dynamiky scény. Statické zábery z interiérov prinášajú podstatne menší objem dát než zábery z exteriéru s premennými svetelnými podmienkami a pohybom. Rovnako sa ukázalo, že niektoré kamery so vstavanými optimalizačnými algoritmami ako napríklad Zipstream, vykazovali efektívnejšie využitie dátovej kapacity bez straty obrazovej kvality. Tieto zistenia slúžia ako podklad pre presnejšie zaradenie systémov z pohľadu kapacity úložiska a prenosovej infraštruktúry a budú ďalej využité pri výpočte celkových nákladov na životný cyklus kamier.

Tabuľka 14 Porovnanie kamier podľa dátovej náročnosti

Kamera	Interiér (statický) [MB/h]	Exteriér (pohyb) [MB/h]	Premenlivé svetlo [MB/h]
AXIS M1045- LW	715,36	1 674,02	1 962,91
AXIS Q1635	1 496,19	3 613,56	4 201,51
AXIS P1435-LE	1 226,29	2 718,93	3 271,22
AXIS P3225- LVE Mk II	1 084,84	2 387,66	3 000,63
AXIS Q3505-V	1 313,39	2 994,61	3 750,86

(zdroj: vlastný)

8.3 Dáta generované za deň a mesiac

Na základe údajov uvedených v Tabuľke 14 bolo následne vykonané stanovenie množstva dát, ktoré sú jednotlivými kamerami generované počas nepretržitej 24 hodinovej a 30 dňovej prevádzky. Tento výpočet bol realizovaný s cieľom posúdiť kapacitné nároky na úložisko v reálnych prevádzkových podmienkach a vytvoriť podklad pre výpočet súvisiacich nákladov v modeli TCO. Pri výpočte sa vychádzalo z hodnôt dátovej náročnosti zistených v scenári s premenlivým svetlom, ktorý počas testovania vykazoval najvyšší objem generovaných dát. Tento prístup umožnil identifikovať maximálne možné zaťaženie úložiska z pohľadu jednej kamery pri nepretržitej prevádzke. Objem dát generovaný za deň bol vypočítaný ako súčin hodinovej dátovej náročnosti a 24 hodín v jednom dni. Následne bol prevedený na gigabajty. Mesačný objem bol vypočítaný ako násobok denného objemu a tridsiatich dní. Prepočet bol realizovaný podľa nasledovných vzorcov:

$$\text{Denný objem [GB]} = \frac{\text{Dátová náročnosť} \left[\frac{\text{MB}}{\text{h}} \right] * 24 [\text{hodín}]}{1\,024};$$

$$\text{Mesačný objem [GB]} = \text{Denný objem [GB]} * 30[\text{dní}].$$

Je potrebné si uvedomiť, že počet dní v jednotlivých mesiacoch nie je rovnaký, avšak pre účely tohto výpočtu bola zvolená zaokrúhlená hodnota 30 dní, ktorá umožňuje jednoduchý a jednotný výpočet pre všetky kamerové modely. Výsledky výpočtu sú uvedené v nasledujúcej tabuľke, ktorá sumarizuje množstvo dát generovaných každou testovanou kamerou za deň a za mesiac.

Tabuľka 15 Denný a mesačný objem dát na kameru

Kamera	Denný objem dát [GB]	Mesačný objem dát [GB]
AXIS M1045-LW	46,01	1 380,3
AXIS Q1635	98,47	2 954,1
AXIS P1435-LE	76,67	2 300,1
AXIS P3225-LVE Mk II	70,33	2 109,9
AXIS Q3505-V	87,91	2 637,3

(zdroj: vlastný)

9 VÝPOČET NÁKLADOV NA ENERGIU A ÚLOŽISKO

V tejto kapitole sa uvádzajú odhady nákladov spojených s dlhodobou prevádzkou vybraných bezpečnostných kamier testovaných v predchádzajúcich častiach práce. Výpočty sú rozdelené do dvoch hlavných kategórií a to náklady na spotrebu elektrickej energie a náklady na úložisko záznamov. Cieľom tejto časti je ukázať, aký vplyv má technická náročnosť kamier na prevádzkový rozpočet počas ich životnosti a aké rozdiely môžu nastať v závislosti od typu zariadenia.

9.1 Výpočet nákladov na elektrickú energiu

Na základe predchádzajúcich meraní príkonu jednotlivých kamier počas aktívneho záznamu boli vypočítané odhadované náklady na elektrickú energiu pri ich dlhodobej nepretržitej prevádzke. Vstupné hodnoty príkonu boli spracované tak, aby bolo možné určiť spotrebu za deň aj za celý rok. Denná spotreba elektrickej energie bola určená podľa vzorca:

$$\text{Denná spotreba [kWh]} = \frac{\text{Priemerný výkon [W]} * 24 [\text{dní}]}{1\,000};$$

kde číslo 24 predstavuje počet hodín v jednom dni, teda ide o výpočet spotreby pri celodennej prevádzke. Príkon v jednotkách W bol týmto vynásobený a následne delený číslom 1000, čím bola hodnota prevedená na kWh, ktoré sú štandardnou jednotkou účtovanou v cenníkoch dodávateľov elektrickej energie. Ročný náklad na elektrickú energiu bol následne vypočítaný ako:

$$\text{Ročný náklad na energiu [€]} = \text{Denná spotreba [kWh]} * 365[\text{dní}] * 0,20[\text{€}];$$

kde číslo 365 predstavuje počet dní v roku a 0,20 € je predpokladaná cena jednej kilowatthodiny elektriny, ktorá bola zvolená na základe priemerných cien pre domácnosti v Českej republike. Cena zahŕňa všetky zložky konečnej sadzby vrátane distribučných poplatkov a daní. Takto vypočítané hodnoty sú uvedené v Tabuľke 16. Porovnaním jednotlivých kamier možno pozorovať významné rozdiely v nákladoch spôsobené odlišným príkonom zariadení. Kamera AXIS Q1635 patrí medzi energeticky náročnejšie, zatiaľ čo model AXIS M1045-LW vykazuje najnižšiu spotrebu a s ňou súvisiaci minimálny náklad na elektrinu.

Uvedené ročné náklady na elektrickú energiu predstavujú odhad pre jeden rok prevádzky. V prípade, že sa hodnotí celkový vplyv na náklady počas celej životnosti systému, je potrebné s týmto výdavkom počítať opakovane za každý rok prevádzky. Taktiež

sa v uvedených výpočtoch nepočítalo s drobnými stratami vznikajúcimi pri napájaní cez PoE, napríklad na odporoch káblového vedenia. Tieto hodnoty sú v praxi zanedbateľné a nemajú výrazný vplyv na výslednú spotrebu v meranom rozsahu.

9.2 Výpočet nárokov na úložisko

Dátová náročnosť kamier bola stanovená na základe meraní veľkostí výstupného videozáznamu v režime s premenlivým osvetlením, ktorý predstavuje najnáročnejšiu prevádzkovú situáciu z hľadiska objemu generovaných dát. Výsledky boli udávané v MB/h a slúžili ako vstupné údaje pre výpočet dennej a ročnej potreby úložiska. Výpočet bol realizovaný podľa rovnice:

$$\text{Denný záznam [GB]} = \frac{\text{Dátová náročnosť} \left[\frac{\text{MB}}{\text{h}} \right] * 24[\text{hodín}]}{1\,024};$$

kde číslo 24 vyjadruje počet hodín záznamu za deň a 1024 je použité na prevod megabajtov na gigabajty. Ročná spotreba úložiska bola následne vypočítaná ako:

$$\text{Ročná potreba úložiska [TB]} = \frac{\text{Denný záznam [GB]} * 365[\text{dní}]}{1\,024};$$

kde číslo 365 zodpovedá počtu dní v roku, pričom ďalším delením číslom 1024 bola hodnota prevedená z gigabajtov na terabajty.

Získané hodnoty boli následne využité pre výpočet nákladov na úložisko pri dvoch typoch riešení ktorými sú náklady pri použití lokálneho úložiska a pri využití cloudových služieb. Pre potreby modelu bola cena za 1 TB dátového priestoru stanovená orientačne. V prípade lokálneho úložiska bola použitá hodnota 40 € za 1 TB úložnej kapacity na jeden rok, ktorá zodpovedá priemernej hodnote odvodennej z cien bežných (Network Attached Storage) ďalej už len ako NAS diskov pri predpoklade ich päťročnej životnosti. V prípade cloudového riešenia bola zvolená hodnota 100 € za 1 TB na rok, čo vychádza z priemerných cien komerčne dostupných služieb určených na dlhodobé uchovávanie videozáznamov v oblasti bezpečnostných technológií. Je však potrebné poznamenať, že tieto ceny nie sú jednotné a v praxi sa môžu v závislosti od poskytovateľa, rozsahu služieb alebo úrovne zabezpečenia líšiť.

Ročné náklady na úložisko boli vypočítané samostatne pre obe uvažované riešenia a to fyzický disk a cloudové služby. V prípade lokálneho úložiska pevného disku (Hard Disk Drive) ďalej už len ako HDD, bola celková ročná potreba dát v TB vynásobená jednotkovou

cenou 40 € za 1 TB. Pri cloudovom riešení bola použitá cena 100 € za 1 TB. Výpočty boli realizované podľa rovníc:

$$\text{Ročný náklad na HDD [€]} = \text{Ročná potreba úložiska [TB]} * 40 \text{ [€]};$$

$$\text{Ročný náklad na cloud [€]} = \text{Ročná potreba úložiska [TB]} * 100 \text{ [€]}.$$

Týmto spôsobom boli vypočítané celkové ročné náklady na uchovávanie videozáznamu pri jednotlivých kamerových modeloch. Výsledné hodnoty sú uvedené v Tabuľke 16. Tá umožňuje porovnať jednotlivé modely z hľadiska prevádzkových nákladov a predstavuje vstup do následného modelu TCO.

Tabuľka 16 Porovnanie nákladov kamier

Kamera	Denná spotreba [kWh]	Ročný náklad na energiu [€]	Denný záznam [GB]	Ročná potreba úložiska [TB]	Ročný náklad na HDD	Ročný náklad na cloud [€]
AXIS M1045-LW	0,0768	5,61	46,01	16,4	656	1 640
AXIS Q1635	0,228	16,64	98,47	35,1	1 404	3 510
AXIS P1435-LE	0,18	13,14	76,67	27,33	1 093,2	2 733
AXIS P3225-LVE Mk II	0,1488	10,86	70,33	25,07	1 002,8	2 507
AXIS Q3505-V	0,168	12,26	87,91	31,34	1 253,6	3 134

(zdroj: vlastný)

Z Tabuľky 16 možno vyvodiť, že medzi testovanými kamerami existujú výrazné rozdiely v prevádzkových nákladoch, ako z hľadiska spotreby elektrickej energie, tak aj z požiadaviek na úložisko. Zariadenie AXIS Q1635 patrí medzi energeticky aj dátovo najnáročnejším modelom, čo sa priamo premieta do jeho ročného nákladu na elektrinu aj uchovávanie videozáznamov. Oproti tomu model AXIS M1045-LW vykazuje najnižšiu

spotřebu aj objem dát, tým pádom generuje celkovo najnižšie prevádzkové náklady. Tieto rozdiely môžu mať pri veľkých kamerových systémoch významný vplyv na celkový rozpočet a mali by byť zohľadnené už v plánovacej fáze projektu.

10 POROVNANIE ZARIADENÍ Z HĽADISKA NÁROČNOSTI

Táto kapitola sa venuje porovnaniu testovaných kamerových zariadení z hľadiska ich prevádzkovej náročnosti. Výsledky meraní a výpočtov uvedených v predchádzajúcich častiach boli spracované a interpretované tak, aby bolo možné identifikovať rozdiely medzi jednotlivými modelmi z pohľadu dlhodobých nákladov. Zámerom je poskytnúť čitateľovi prehľad o tom, ktoré zariadenia sú z hľadiska spotreby energie a objemu generovaných dát výhodnejšie a ktoré môžu byť finančne náročnejšie pri dlhodobom nasadení. Porovnanie bolo zamerané na tri základné ukazovatele, ktoré predstavujú jadro prevádzkových nákladov, konkrétne ročná spotreba elektrickej energie, ročný objem vygenerovaných dát a z toho vyplývajúci náklad na cloudové úložisko. Všetky tieto veličiny boli vypočítané na základe predchádzajúcich meraní a zohľadňujú nepretržitú 24 hodinovú prevádzku kamier počas celého roka. Ročná spotreba elektrickej energie bola určená podľa vzorca:

$$\text{Ročná spotreba [kWh]} = \frac{\text{Priemerný výkon [W]} * 24 [\text{hodín}] * 365 [\text{dní}]}{1000};$$

kde číslo 24 predstavuje počet hodín v jednom dni, teda ide o výpočet spotreby pri celodennej prevádzke. Násobením hodnotou 365 sa zohľadňuje počet dní v roku, čo umožňuje určiť celkovú spotrebu za celé obdobie jedného kalendárneho roka. Výsledná hodnota v jednotkách wathodina bola následne delená číslom 1000, čím bola prevedená na kilowathodiny, ktoré predstavujú štandardnú jednotku používanú pri fakturácii elektrickej energie. Objem dát v TB bol vypočítaný prepočtom z meranej hodnoty dátovej náročnosti v MB/h. Prevod bol realizovaný vzorcom:

$$\text{Ročný objem dát [TB]} = \frac{\frac{\text{MB}}{\text{h}} * 24 [\text{hodín}] * 365 [\text{dní}]}{1024^2};$$

kde číslo 24 opäť predstavuje počet hodín v jednom dni a číslo 365 počet dní v roku. Výsledkom násobenia je celkové množstvo dát vygenerované za rok, udané v megabajtoch. Táto hodnota bola následne dvakrát delená číslom 1024, prvýkrát na prevod z MB na GB a druhý krát na prevod z GB na TB, čím sa získala požadovaná jednotka objemu dát vhodná pre vyhodnocovanie ročnej kapacity úložiska. Ročný náklad na cloudové úložisko bol stanovený podľa vzorca:

$$\text{Ročný náklad na cloud [€]} = \text{Ročný objem dát [TB]} * 100 [\text{€}];$$

kde 100 € na TB bola zvolená ako orientačná priemerná cena cloudového priestoru určeného na uchovávanie videozáznamov v oblasti bezpečnostných technológií.

Tabuľka 17 sumarizuje uvedené údaje pre všetky porovnávané kamerové modely. Umožňuje jednoduché porovnanie a zároveň tvorí podklad pre následné hodnotenie efektívnosti systémov v rámci TCO modelu.

Tabuľka 17 Porovnanie kamier podľa náročnosti

Kamera	Ročná spotreba (kWh)	Ročný objem dát (TB)	Ročný náklad na cloud (€)
AXIS M1045-LW	28,03	16,4	1 640
AXIS Q1635	83,22	35,1	3 510
AXIS P1435-LE	65,7	27,33	2 733
AXIS P3225-LVE Mk II	54,31	25,07	2 507
AXIS Q3505-V	61,32	31,34	3 134

(zdroj: vlastný)

Z tabuľky vyplýva, že najnáročnejším modelom vo všetkých sledovaných parametroch je AXIS Q1635. Ten dosahuje najvyššiu spotrebu elektrickej energie aj najväčší objem generovaných dát, čo sa priamo odráža v najvyššom ročnom náklade na cloudové úložisko. Naopak, model AXIS M1045-LW patrí medzi najúspornejšie kamery a vykazuje najnižšiu spotrebu aj produkciu dát. Je preto vhodným riešením pre aplikácie, kde je rozhodujúcim kritériom minimalizácia prevádzkových nákladov. Rozdiely medzi jednotlivými kamerami sú z pohľadu dlhodobej prevádzky podstatné a pri väčších systémoch sa môžu výrazne premietnuť do celkového rozpočtu. Z tohto dôvodu by mali byť tieto faktory zohľadnené už vo fáze návrhu a výberu technológie.

11 INTERPRETÁCIA VÝSLEDKOV A ODPORÚČANIA

Na základe vykonaných meraní spotreby elektrickej energie, vyhodnotenia veľkosti videozáznamov a výpočtov nákladov na úložisko boli jednotlivé kamery vyhodnotené z hľadiska ich celkovej ročnej prevádzkovej náročnosti. Zistené hodnoty boli následne spracované do sumarizačnej tabuľky, ktorá zachytáva ročné náklady na cloudové úložisko, ročné náklady na energiu a ich súčet. Tento súčet bol označený ako celkové ročné náklady, pričom ide o jeden z kľúčových výstupov praktickej časti práce. Výsledky ukázali, že najnáročnejším modelom z pohľadu kombinovaných nákladov na úložisko a elektrickú energiu je kamera AXIS Q1635. Jej vysoká dátová náročnosť bola spôsobená najmä technickými parametrami, ako je vyššie rozlíšenie, rýchlosť snímkovania a citlivosť na zmeny scény, čo sa prejavilo v generovaní väčšieho objemu dát. Zároveň bola zaznamenaná aj vyššia priemerná spotreba elektrickej energie. V dôsledku toho tento model dosiahol najvyšší ročný náklad na úložisko aj energiu. Naopak najúspornejšou kamerou sa ukázal model AXIS M1045-LW, ktorý dosahoval najnižšie hodnoty vo všetkých sledovaných parametroch. Jeho technická jednoduchosť, nižší prín a nižší dátový tok viedli k výrazne nižšiemu objemu dát aj minimálnej spotrebe energie. Tento model je preto vhodný najmä pre priestory s nižšími nárokmi na rozlíšenie a kvalitu záznamu.

Z hľadiska návrhu a optimalizácie bezpečnostných systémov sa na základe týchto výsledkov odporúča zohľadniť niekoľko zásad. V prostrediach, kde nie je vyžadované vysoké rozlíšenie alebo vysoká snímková frekvencia, je vhodné uprednostniť menej dátovo náročné modely, čím sa dosiahnu úspory najmä pri využívaní cloudového úložiska. Pri rozsiahlejších inštaláciách je vhodné zvážiť aj kombináciu rôznych typov kamier, napríklad jednoduchšie modely v interiéri a výkonnejšie zariadenia na kritických bodoch v exteriéri. Zároveň sa odporúča využiť funkcie inteligentného záznamu, ako je nahrávanie pri detekcii pohybu, ktoré dokážu významne znížiť objem dát. V prípade obmedzeného rozpočtu je možné zvážiť aj využitie lokálneho úložiska namiesto cloudového riešenia.

11.1 Výpočet celkových ročných nákladov

Na výpočet celkových ročných nákladov boli použité hodnoty, ktoré boli získané a vypočítané v predchádzajúcich častiach práce. Ročné náklady na cloudové úložisko aj náklady na elektrickú energiu boli stanovené osobitne pre každý kamerový model na základe reálnych meraní a následných výpočtov.

Tieto dve hodnoty boli následne sčítané, aby bol získaný prehľad o celkovej ročnej finančnej záťaži spojenej s prevádzkou jednej kamery. Použitý výpočtový vzorec mal nasledovný tvar:

$$\text{Celkové ročné náklady [€]} = \text{Ročné náklady na energiu [€]} + \text{Ročné náklady na úložisko [€]}.$$

Hodnoty vstupných premenných sú známe z predchádzajúcich výpočtových tabuliek, kde boli ročné náklady na energiu odvodené na základe meraného príkonu kamier a predpokladanej 24 hodinovej prevádzky. Ročné náklady na úložisko boli vypočítané ako súčin ročného objemu dát a jednotkovej sadzby 100 € za 1 TB dátového priestoru ročne. Tabuľka 18 sumarizuje celkové ročné náklady pre všetky testované modely. Tieto údaje predstavujú praktický základ pre výber kamier pri zostavovaní rozpočtu bezpečnostného systému z pohľadu dlhodobej efektivity.

Tabuľka 18 Porovnanie ročných nákladov kamier

Kamera	Ročné náklady na úložisko (€)	Ročné náklady na energiu (€)	Celkové ročné náklady (€)
AXIS M1045-LW	1 640	5,61	1 645,6
AXIS Q1635	3 510	16,64	3 526,6
AXIS P1435-LE	2 733	13,14	2 746,1
AXIS P3225-LVE Mk II	2 507	10,86	2 517,9
AXIS Q3505-V	3 134	12,26	3 146,3

(zdroj: vlastný)

12 PREPOJENIE VÝSLEDKOV S TCO MODELOM

V tejto časti práce boli praktické výsledky získané meraním prepojené s teoretickým rámcom modelu TCO, ktorý bol predstavený v úvodných kapitolách. TCO predstavuje metodiku slúžiacu na komplexné zhodnotenie finančných nákladov spojených s technológiou počas celého jej životného cyklu od počiatočného obstarania až po jej vyradenie z prevádzky. Na základe meraní spotreby elektrickej energie a dátovej náročnosti boli pre každý kamerový model vypočítané ročné prevádzkové náklady. Tieto náklady zahŕňajú náklady na energiu, náklady na cloudové úložisko a predpokladané výdavky na údržbu a servis. Hodnoty ročných nákladov na elektrickú energiu a úložisko boli vzhľadom na ich spracovanie v predchádzajúcich častiach práce z tabuľky vynechané, aby sa predišlo opakovaniu údajov. Výpočet celkových prevádzkových nákladov bol realizovaný podľa vzorca:

$$\text{Celkový OpEx [€]} = (\text{Energia}_{\text{Rok}} [\text{€}] + \text{Úložisko}_{\text{Rok}} [\text{€}] + \text{Údržba}_{\text{Rok}} [\text{€}]) * \text{Životnosť [rok]}.$$

Ročné náklady na energiu a úložisko boli prevzaté z predchádzajúcich výpočtov, kde vychádzali z meraných hodnôt spotreby a dátovej náročnosti jednotlivých kamier. Ročné náklady na údržbu boli stanovené odhadom na základe typu a zložitosti jednotlivých zariadení. Pre jednoduchšie modely bola predpokladaná hodnota 60 €, pri komplexnejších zariadeniach sa počítalo s výdavkami vo výške 80 € ročne. Tento predpoklad zahŕňa náklady na pravidelné revízie, čistenie, aktualizácie firmvéru alebo výmenu drobných komponentov. Pri výpočte celkových nákladov na úložisko sa zároveň uvažovalo s tým, že všetky záznamy sú uchovávané nepretržite počas celého roka bez pravidelného premazávania. Tento predpoklad výrazne ovplyvnil výslednú výšku ročných nákladov, ktoré dosahujú vysoké hodnoty najmä pri kamerách s vyššou dátovou náročnosťou. V reálnych inštaláciách býva však často uplatňovaný prístup, pri ktorom sa staršie záznamy pravidelne premazávajú ako napríklad v intervale 7, 14 alebo 30 dní, čím sa znižujú požiadavky na úložnú kapacitu a zároveň aj súvisiace náklady. Takéto nastavenie sa využíva predovšetkým v systémoch s obmedzeným rozpočtom alebo v prípadoch, keď sa uchovávanie záznamov vyžaduje len krátkodobo, napríklad na účely operatívnej bezpečnosti. Pri výpočtoch nákladov na úložisko sa zámerne uvažovalo s cloudovým riešením, a to najmä z dôvodu jeho výhod v oblasti bezpečnosti, vzdialeného prístupu, škálovateľnosti a nižších nárokov na údržbu. Tento prístup zároveň lepšie odráža aktuálne trendy v oblasti IP dohľadových systémov, kde sa cloudové úložiská uprednostňujú pred tradičnými lokálnymi diskovými riešeniami. Životnosť kamier bola pre účely porovnania stanovená jednotne na päť rokov. Táto hodnota

zodpovedá technickému cyklu obvyklému pre bezpečnostné kamery používané v praxi, pri ktorých sa počas tohto obdobia predpokladá plnohodnotná funkcia bez potreby výmeny celého zariadenia. Hodnota TCO bola určená súčtom investičných a celkových prevádzkových výdavkov:

$$TCO [\text{€}] = CapEx [\text{€}] + \text{Celkový } OpEx [\text{€}].$$

Kapitálové náklady (CapEx) boli stanovené podľa orientačných trhových cien platných pre jednotlivé kamerové modely. Uvažovalo sa s cenami bez Dane Pridanej Hodnoty, ďalej už len ako DPH, ktoré sa môžu v praxi líšiť v závislosti od viacerých faktorov, ako sú objem odberu, zľavová politika dodávateľov, aktuálna dostupnosť na trhu či kurzové rozdiely pri dovoze zariadení. Tieto ceny sa vzťahovali výhradne na kameru a základné príslušenstvo, bez zahrnutia nákladov na montáž alebo sieťovú infraštruktúru. Týmto spôsobom boli zabezpečené porovnateľné vstupné podmienky pre všetky analyzované zariadenia. Všetky hodnoty boli spracované do Tabuľky 19, ktorá poskytuje prehľad o jednotlivých zložkách nákladov a umožňuje priame porovnanie efektívnosti modelov z hľadiska celkových nákladov počas životného cyklu.

Tabuľka 19 TCO kamier

Kamera	CapEx (€)	Údržba a servis ročne (€)	Odhadovaná životnosť (roky)	Celkový OpEx (€)	TCO (€)
AXIS M1045-LW	237	60	5	8 528,1	8 765,1
AXIS Q1635	1247	80	5	18 033	19 280
AXIS P1435-LE	670	60	5	14 031	14 701
AXIS P3225-LVE Mk II	756	80	5	12 989	13 745
AXIS Q3505-V	927	80	5	16 131	17 058

(zdroj: vlastný)

13 MERANIE SPOTREBY ELEKTRICKEJ ENERGIE ÚSTREDNE A PERIFÉRNÝCH ZARIADENÍ

Okrem analýzy spotreby elektrickej energie jednotlivých IP kamier bola vykonaná samostatná analýza zameraná na spotrebu zabezpečovacej ústredne a k nej pripojených periférnych zariadení. Meranie bolo realizované v stave, ktorý simuloval bežnú reálnu prevádzku systému a to s aktívnymi detektormi, signalizačnými prvkami a plne funkčným riadiacim centrom. Na meranie bol použitý wattmeter Solight DT26, ktorý umožňuje sledovanie okamžitého odberu elektrickej energie a napätia, ako aj kumulatívnej spotreby v kWh. Meranie bolo zamerané na súhrnný príkon celej zostavy v základnom pohotovostnom režime, bez aktivácie alarmu či výstupných komponentov.

Do systému boli zapojené nasledujúce prvky:

- **zabezpečovacia ústredňa s akumulátorom a napájacím modulom** – ľavý horný roh, otvorená skrinka;
- **pasívne infračervené detektory pohybu (PIR)** – dva detektory v pravej hornej časti;
- **opticko-dymový detektor** – pravý horný roh;
- **magnetické kontakty** – spodná stredná časť panela;
- **klávesnica a stavové LED indikátory** – vľavo dole so signalizáciou stavu a zón;
- **bezkontaktná čítačka pre ovládanie systému pomocou (Radio-Frequency Identification) RFID kľúčienky** – vľavo dole;
- **teplotný displej** – digitálny, napravo od čítačky;
- **LED diódy** – stredná ľavá časť panelu;
- **piezoelektrická siréna** – spodný pravý roh;
- **reléové a bezdrôtové moduly** – dolný pravý roh (červená súčiastka na doske plošného spoja;
- **napájací zdroj s batériovým zálohovaním** – integrovaný v ústredni.



Obrázok 22 Zabezpečovacia ústredňa
so zapojenými periférnymi zariadeniami

(zdroj: vlastný)

Na základe merania zabezpečovacej ústredne a pripojených periférnych zariadení bola vypočítaná priemerná denná, mesačná a ročná spotreba elektrickej energie. Priemerný príkon zariadenia bol priamo odčítaný z meracieho zariadenia a dosahoval hodnotu 5,83 W. Následne bola podľa tejto hodnoty dopočítaná denná spotreba v kWh, ktorá bola v ďalšom kroku prenasobená počtom dní v mesiaci a roku. Denná spotreba bola vypočítaná podľa vzorca:

$$E_{deň} [kWh] = \frac{P [W] * 24 [hodín]}{1000};$$

kde P predstavuje príkon vo wattoch, číslo 24 zodpovedá počtu hodín v jednom dni a delením číslom 1000 sa vykonala konverzia z Wh na kWh. Mesačná a ročná spotreba boli stanovené nasledovne:

$$E_{mesiac} [kWh] = E_{deň} [kWh] * 30 [dní];$$

$$E_{rok} [kWh] = E_{deň} [kWh] * 365 [dní];$$

kde číslo 30 predstavuje počet dní v mesiaci a číslo 365 počet dní v roku. Pri výpočte mesačnej spotreby sa uvažovalo so štandardizovaným počtom 30 dní v mesiaci, čím sa dosiahla jednoduchšia a jednotná porovnateľnosť medzi rôznymi typmi zariadení. Tento prístup zároveň zjednodušuje následné ekonomické prepočty v rámci modelu TCO.

Tabuľka 20 Spotreba ústredne a periférií

Zariadenie	Príkon (W)	Denná spotreba (kWh)	Mesačná spotreba (kWh)	Ročná spotreba (kWh)
Zabezpečovacia ústredňa + periférie	5,83	0,14	4,2	51,1

(zdroj: vlastný)

Na základe uvedenej spotreby elektrickej energie zabezpečovacej ústredne a jej periférií bola stanovená výška denného, mesačného a ročného nákladu na elektrickú energiu. Výpočet bol realizovaný podľa vzorca:

$$\text{Náklad [€]} = E [\text{kWh}] * c \left[\frac{\text{€}}{\text{kWh}} \right];$$

kde E predstavuje spotrebu elektrickej energie v kWh (dennú, mesačnú alebo ročnú) a c je jednotková cena elektriny. Pri výpočtoch sa uvažovalo jednotkovou cenou elektrickej energie vo výške 0,20€/kWh, ktorá zodpovedá priemernej cene pre domácnosti. Výsledné hodnoty sú uvedené v nasledujúcej tabuľke.

Tabuľka 21 Náklady na elektrickú energiu ústredne a jej periférií

Zariadenie	Denný náklad [€]	Mesačný náklad [€]	Ročný náklad [€]
Zabezpečovacia ústredňa a jej periférie	0,03	0,84	10,22

(zdroj: vlastný)

14 ZHRNUTIE A INTERPRETÁCIA VÝSLEDKOV TCO PRE CELÝ SYSTÉM PZTS

V tejto časti sú analyzované výsledky TCO získané aplikáciou predstaveného matematického modelu a evaluačného algoritmu na vybrané bezpečnostné technológie. Analýza sa zameriava na identifikáciu nákladových položiek a porovnanie celkovej ekonomickej náročnosti rôznych komponentov a modelových scenárov.

14.1 Rekapitulácia výsledkov TCO podľa modelových scenárov

Na základe definovaného algoritmu boli vypočítané hodnoty TCO pre jednotlivé testované kamery a modelové scenáre. Pre VSS komponenty boli použité dáta z Tabuľky 19, ktorá sumarizuje CapEx, odhadovanú údržbu a celkové OpEx počas 5 ročnej životnosti. Pre PZTS sa vychádzalo z nameranej spotreby energie v Tabuľke 21 a odhadovaných CapEx a nákladov na údržbu, ako bolo demonštrované v príklade scenára 2 v kapitole 5.3.3.

Súhrn výsledkov TCO (príklady):

scenár 1 pre TCO jednotlivých kamier za 5 rokov;

- AXIS M1045-LW – 8765,1 €;
- AXIS Q1635 – 19280 €;
- AXIS P1435-LE – 14701 €;
- AXIS P3225-LVE Mk II – 13745 €;
- AXIS Q3505-V – 17058 €;

scenár 2 pre integrovaný systém;

- TCO (kamera P1435-LE) – 14701 €;
- TCO PZTS – 476,1 €;
- Celkové TCO (scenár 2) – 14 701 € + 476,1 € = 15 177,1 €.

14.2 Analýza nákladových zložiek TCO

Analýza ukazuje, že štruktúra TCO sa výrazne líši medzi VSS a PZTS a tiež medzi jednotlivými modelmi kamier.

1. CapEx:

- pre VSS predstavujú obstarávacie ceny kamier, popísané v Tabuľke 19, významnú počiatočnú investíciu, pohybujúcu sa od 237 € (AXIS M1045-LW) až po 1247 € (AXIS Q1635);
- pre PZTS bol CapEx v modeli odhadovaný, keďže v praktickej časti nebol presne vyčíslený pre celý systém PZTS.

2. OpEx:

- náklady na cloudové úložisko sú dominantnou zložkou OpEx a celkového TCO pre všetky testované kamery. Napríklad pre AXIS M1045-LW tvoria ročné náklady na cloudové úložisko 1640 €, čo za 5 rokov predstavuje 8200 €. Toto je výrazne viac ako samotný CapEx kamery (237 €). Tento fakt je spôsobený predpokladom kontinuálneho ukladania dát počas celého roka pri cene 100 € / TB / rok;
- náklady na elektrickú energiu sú relatívne nízke pre VSS aj PZTS. Ročné náklady na energiu pre kamery sa pohybujú od 5,61 € (AXIS M1045-LW) do 16,64 € (AXIS Q1635). Pre PZTS ústredňu s perifériami sú ročné náklady na energiu približne 10,22 €. Tieto náklady teda nepredstavujú kritický faktor v celkovom TCO;
- náklady na údržbu kamier boli odhadnuté na 60 € až 80 € ročne. Za 5 rokov to predstavuje 300 € až 400 €, čo je významná, no nie dominantná položka v porovnaní s nákladmi na úložisko. Pre PZTS bola údržba odhadovaná.

Podiel OpEx na celkovom TCO je pri VSS extrémne vysoký, najmä kvôli nákladom na cloudové úložisko pri zvolených predpokladoch. Napríklad AXIS M1045-LW je CapEx 237 €, zatiaľ čo celkový OpEx za 5 rokov je 8 528,1 €.

14.3 Porovnanie komponentov a scenárov

Porovnanie VSS:

- najnižšie TCO (8 765,1 €) vykazuje model AXIS M1045-LW, a to vďaka nízkemu CapEx a najnižším nákladom na energiu a úložisko;
- najvyššie TCO (19 280 €) má model AXIS Q1635, čo je spôsobené vysokým CapEx a najvyššími nákladmi na energiu a úložisko v dôsledku vysokej dátovej náročnosti a spotreby.

Analýza integrovaného scenára (VSS+PZTS):

- v modelovom scenári 2 je celkové TCO 15 177,1 €;
- dominantnú časť nákladov tvorí VSS komponent (TCO kamery 14 701 €), zatiaľ čo TCO pre PZTS (476,1 € pri daných odhadoch) je podstatne nižšie.

14.4 Vplyv kľúčových parametrov a citlivosť modelov

- Cena úložiska – tento parameter má najzásadnejší vplyv na TCO VSS. Zmena ceny za TB/rok by dramaticky ovplyvnila výsledky. Použitie lokálneho NAS úložiska s cenou 40 € / TB / rok by výrazne znížilo náklady na úložisko oproti cloudovému riešeniu za 100 € / TB / rok.
- Dĺžka archivácie záznamov – model predpokladal kontinuálne ukladanie počas celého roka. V praxi sa často záznamy uchovávajú kratšiu dobu ako napríklad 7, 14 alebo 30 dní. Skrátenie doby archivácie by radikálne znížilo požiadavky na kapacitu úložiska a tým aj náklady, čo by zmenilo celkové TCO a pomery medzi jednotlivými nákladovými zložkami.
- Použitie inteligentného záznamu – nahrávanie len pri detekcii pohybu namiesto kontinuálneho záznamu by taktiež významne znížilo objem dát a náklady na úložisko.
- Cena elektrickej energie – vzhľadom na nízky podiel nákladov na energiu by aj výraznejšia zmena ceny elektrickej energie mala len malý dopad na celkové TCO.
- Životnosť systému – predĺženie alebo skrátenie predpokladanej 5 ročnej životnosti by priamo úmerne zmenilo celkové prevádzkové náklady a tým aj TCO.

14.5 Obmedzenia aplikovaného modelu

Je dôležité si uvedomiť, že prezentovaný model TCO je zjednodušením reality a je založený na dostupných dátach z praktickej časti práce.

- Nezahrnuté náklady – model explicitne nekvantifikuje všetky potencionálne náklady, ako sú detailné náklady na inštaláciu a konfiguráciu (mimo ceny hardvéru), softvérové licencie, náklady na komplexné školenia personálu, náklady na sieťovú infraštruktúru, náklady na likvidáciu systému či skryté náklady spojené s prestojmi alebo falošnými poplachmi. Tieto faktory sú vymenované v Tabuľke 11, ale neboli číselne zahrnuté do výpočtov TCO v konkrétnom modeli.
- Odhady – niektoré vstupné údaje, ako ročné náklady na údržbu kamier a najmä CapEx a údržba pre PZTS, sú založené na odhadoch alebo orientačných trhových cenách. Presnosť TCO je priamo závislá od presnosti týchto vstupov.
- Špecifické podmienky – výpočty dátovej náročnosti a spotreby energie boli vykonané za špecifických podmienok testovania. V iných prevádzkových podmienkach sa môžu tieto hodnoty líšiť.

14.6 Závery a praktické odporúčania vyplývajúce z analýzy

Analýza výsledkov získaných algoritmom potvrdzuje, že:

- náklady na úložisko sú kritické. Pri systémoch VSS, najmä pri použití cloudového úložiska a kontinuálneho záznamu, tvoria náklady na úložisko dominantnú časť TCO. Optimalizácia v tejto oblasti je kľúčová pre zníženie celkových nákladov;
- CapEx nie je všetko. Najlacnejšia kamera z hľadiska obstarávacej ceny bola najlacnejšia aj z hľadiska TCO vďaka nízkej dátovej a energetickej náročnosti, avšak pri porovnaní iných modelov by sa mohlo ukázať, že vyšší CapEx za kameru s lepšou kompresiou dát sa môže vrátiť v nižších nákladoch na úložisko;
- energetická náročnosť je sekundárna. Hoci sú medzi kamerami rozdiely v spotrebe energie, tieto náklady tvoria len malú časť celkového TCO VSS aj PZTS;

- PZTS má výrazne nižšie TCO (pri daných predpokladoch). Samotný systém PZTS, najmä ak sa jeho TCO počíta hlavne z energie a odhadovanej údržby a CapEx, má podstatne nižšie celkové náklady ako VSS komponenty zaťažené vysokými nákladmi na úložisko;
- dôsledný výber technológie je dôležitý. Výber kamier by mal zohľadňovať nielen požadovanú kvalitu obrazu, ale aj dátovú efektivitu a optimalizovaný príkon, aby sa predišlo zbytočne vysokým prevádzkovým nákladom.

Pre kvalifikované rozhodovanie pri návrhu bezpečnostných systémov je nevyhnutné posudzovať náklady komplexne v rámci celého životného cyklu, ako to umožňuje metodika TCO. Tento model, hoci zjednodušený, poskytuje cenný pohľad na štruktúru nákladov a identifikuje oblasti pre potenciálnu optimalizáciu.

ZÁVER

Cieľom tejto bakalárskej práce bolo komplexne sa venovať problematike TCO v kontexte bezpečnostných technológií, konkrétne VSS a PZTS. Tento cieľ bol naplnený prostredníctvom splnenia piatich hlavných bodov zadania a to vypracovania literárnej rešerše, návrhu experimentov, stanovenia faktorov TCO, zhotovenia matematického modelu s evaluačným algoritmom a následného vyhodnotenia a analýzy získaných výsledkov.

V teoretickej časti práce bola detailne spracovaná literárna rešerš týkajúca sa TCO, jeho definície, histórie, metodík výpočtu a faktorov, ktoré ho ovplyvňujú. Zároveň boli popísané základné princípy, komponenty a charakteristiky systémov VSS a PZTS.

V praktickej časti boli navrhnuté a realizované experimenty zamerané na meranie kľúčových parametrov ovplyvňujúcich TCO, konkrétne spotreby elektrickej energie a dátovej náročnosti pre päť vybraných modelov IP kamier AXIS a pre modelovú zostavu PZTS. Na základe týchto meraní a ďalších odhadovaných vstupov ako sú náklady na údržbu a ceny úložiska bol v kapitole 5.3 zhotovený matematický model TCO a praktický evaluačný algoritmus. Tento model bol následne aplikovaný na výpočet TCO pre jednotlivé kamery a pre modelové scenáre, vrátane integrovaného systému VSS a PZTS.

Vyhodnotenie a analýza výsledkov získaných algoritmom, prezentované v kapitole 14, priniesli niekoľko kľúčových zistení. Potvrdilo sa, že pri systémoch VSS tvoria náklady na cloudové úložisko pri predpoklade kontinuálneho záznamu a ročnej archivácie dominantnú časť celkových prevádzkových nákladov a často aj celkového TCO, výrazne prevyšujú počiatkové investičné náklady na hardvér. Náklady na elektrickú energiu sa ukázali byť relatívne nízkou položkou v celkovom TCO pre VSS aj PZTS. Analýza tiež poukázala na významné rozdiely v TCO medzi jednotlivými modelmi kamier, pričom najnižšie TCO vykázal model AXIS M1045-LW a najvyššie model AXIS Q1635. Pri integrovanom systéme VSS a PZTS tvorili náklady na VSS podstatne väčší podiel na celkovom TCO než náklady na PZTS, najmä kvôli nákladom na úložisko VSS.

Analýza citlivosti modelu ukázala, že najväčší vplyv na výsledné TCO VSS má cena úložiska a zvolená dĺžka archivácie záznamov. Skrátenie doby archivácie alebo implementácia inteligentného záznamu by mohli viesť k radikálnemu zníženiu nákladov. Práca taktiež poukázala na obmedzenia aplikovaného modelu, ktorý nezahŕňal všetky potenciálne nákladové položky komplexného TCO z dôvodu zamerania na merateľné a odhadnuteľné faktory v rámci rozsahu práce.

Vypracovaný model TCO a evaluačný algoritmus poskytujú praktický nástroj pre kvalifikovanejší odhad a porovnanie ekonomickej náročnosti bezpečnostných technológií. Výsledky analýzy zdôrazňujú dôležitosť komplexného posudzovania nákladov počas celého životného cyklu a identifikujú kľúčové oblasti pre optimalizáciu.

Pre budúci výskum by bolo prínosné rozšíriť model o ďalšie nákladové faktory, ktoré neboli v tejto práci detailne popísané, ako napríklad detailné náklady na inštaláciu, softvérové licencie či náklady na personál. Taktiež by bolo zaujímavé realizovať merania na širšom portfóliu zariadení od rôznych výrobcov a analyzovať TCO pri rôznych stratégiách archivácie dát a pri použití lokálnych úložných riešení v porovnaní s cloudom. Napriek uvedeným obmedzeniam táto práca poskytuje cenný pohľad na štruktúru nákladov bezpečnostných systémov a potvrdzuje, že dôsledná analýza TCO je nevyhnutným predpokladom pre efektívne investičné rozhodnutia.

ZOZNAM POUŽITEJ LITERATÚRY

- [1] THEASTROLOGYPAGE. *Aké sú celkové náklady na vlastníctvo (tco)? - definícia z technológie.* Online. TheAstrologyPage. 2025. Dostupné z: <https://sk.theastrologypage.com/total-cost-ownership>. [cit. 2025-05-27].
- [2] HOOGENRAAD, Wim. *Celkové náklady na vlastníctvo - TCO.* Online. ITpedia. 30. júla 2017, 6. apríla 2024. Dostupné z: <https://sk.itpedia.nl/2017/07/30/totale-eigendomskosten-tco/>. [cit. 2025-05-27].
- [3] HEILALA, J; HELIN, K a MONTONEN, J. Total cost of ownership analysis for modular final assembly systems. Online. *International Journal of Production Research*. 2011, č. 18-19, article 44, s. 3967-3988. ISSN 0020-7543. Dostupné z: <https://doi.org/10.1080/00207540600806448>. [cit. 2025-05-27].
- [4] CADDI. *Procurement 101: Lifecycle Costing (LCC) – How it works and why it's important.* Online. CADDi. Dostupné z: <https://us.caddi.com/resources/insights/lifecycle-costing#difference-between-tco-and-lcc-2>. [cit. 2025-05-27].
- [5] WETTEMANN, Rebecca. *The Strengths and Weaknesses of TCO.* Online. CSO Online. 2003. Dostupné z: <https://www.csoononline.com/article/511579/data-protection-the-strengths-and-weaknesses-of-tco.html>. [cit. 2025-05-27].
- [6] KNOWLEDGE CENTER. *Total Cost of Ownership: Definition, How to Calculate, and Benefits.* Online. Inbound Logistics. 2024. Dostupné z: <https://www.inboundlogistics.com/articles/total-cost-of-ownership/>. [cit. 2025-05-27].
- [7] PANJAITAN, Donald Sutanto; BAHAGIA, Senator Nur; RAJA, Andi Cakravastia Arisaputra a ABDUH, Muhammad. Total cost of ownership factors in procurement and technology economic assessment: A systematic literature review. Online. *ResearchGate*. S. 1-13. Licence: CC BY 4.0. Dostupné z: <https://doi.org/10.1051/e3sconf/202448401022>. [cit. 2025-05-27].
- [8] HANNA, Katie Terrell, BIGELOW, Stephen J. (ed.). *What is total cost of ownership (TCO)?* Online. TechTarget. 2025. Dostupné z: <https://www.techtarget.com/searchdatacenter/definition/TCO>. [cit. 2025-05-27].

- [9] ADÁMEK, Milan; , Karla; BITALA, Petr; MACH, Václav a ŠEVČÍK, Jiří. *Dohledové videosystémy v bezpečnostních technologiích*. SPBI SPEKTRUM. V Ostravě: ružení požárního a bezpečnostního inženýrství, 2022. ISBN 978-80-7385-263-4.
- [10] ČESKÁ AGENTURA PRO STANDARDIZACI. ČSN EN 62676-1-1, *Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 1-1: Systémové požadavky - Obecně*. Praha: Český normalizační institut, 2014.
- [11] Alicia. *Analog Security Camera: The Ultimate Guide*. Online. Reolink. 2024. Dostupné z: <https://reolink.com/blog/analog-security-camera/>. [cit. 2025-05-27].
- [12] SECURIA PRO. *Výhody a nevýhody inštalácie analógových bezpečnostných kamier*. Online. SECURIA PRO. 2023. Dostupné z: <https://www.securiapro.sk/blog/vyhody-a-nevyhody-instalacie-analogovych-bezpecnostnych-kamier/>. [cit. 2025-05-27].
- [13] SECOM TIPS. *What is Analog Camera? Advantages, Disadvantages and Principle of Operation*. Online. SECOM. 2024. Dostupné z: <https://www.secom.vn/en/column/what-is-an-analog-camera/>. [cit. 2025-05-29].
- [14] LUDWIG, Sarah. *Pro's and Cons for IP vs. Analog Video Surveillance*. Online. Security Magazine. 2018. Dostupné z: <https://www.securitymagazine.com/articles/88854-pros-and-cons-for-ip-vs-analog-video-surveillance?>. [cit. 2025-05-27].
- [15] HAHNE, Wayne. *Pros and Cons On Installing Analog Security Cameras*. Online. A1 SECURITY CAMERAS. 2022. Dostupné z: <https://www.a1securitycameras.com/blog/pros-and-cons-on-installing-analog-security-cameras/>. [cit. 2025-05-29].
- [16] AVILIGON. *A complete guide to IP cameras: definition, types and key features*. Online. AVILIGON. Dostupné z: <https://www.avigilon.com/blog/what-is-an-ip-camera>. [cit. 2025-05-27].
- [17] ŠEVČÍK, Jiří. *Princip činnosti, typy a komunikační rozhraní IP kamer*. Online. 2013. Dostupné z: <https://elektro.tzb-info.cz/10480-princip-cinnosti-typy-a-komunikacni-rozhrani-ip-kamer>. [cit. 2025-05-27].
- [18] TECH BRIEFS. *Modern CMOS Cameras as Replacements for CCD Camera*. Online. Tech Briefs. 2015. Dostupné z: <https://www.techbriefs.com/component/content/article/23094-modern-cmos-cameras-as-replacements-for-ccd-cameras>. [cit. 2025-05-27].

- [19] GILLOT, Tobias. *3 Factors that Influence a Video Surveillance System*. Online. Vocal Media. 2019. Dostupné z: <https://vocal.media/01/3-factors-that-influence-a-video-surveillance-system>. [cit. 2025-05-27].
- [20] DELCORO, Damon. *Factors That Influence a Video Surveillance System*. Online. Security Camera King. Dostupné z: <https://www.securitycameraking.com/securityinfo/factors-that-influence-a-video-surveillance-system/>. [cit. 2025-05-27].
- [21] AXIS COMMUNICATIONS. *AXIS M1045-LW Network Camera: Wireless HDTV 1080p camera with edge storage and IR illumination*. Online. 2021. Dostupné také z: <https://www.axis.com/dam/public/d5/6a/90/datasheet-axis-m1045-lw-network-camera-en-US-276609.pdf>.
- [22] AXIS COMMUNICATIONS. *AXIS Q1635 Network Camera: For details of fast moving objects in difficult lights*. Online. 2019. Dostupné také z: <https://www.axis.com/dam/public/6a/e8/2f/datasheet-axis-q1635-network-camera-en-US-272085.pdf>.
- [23] AXIS COMMUNICATIONS. *AXIS P1435-LE Network Camera: Compact and fully-featured HDTV for any light condition*. Online. 2021. Dostupné také z: <https://www.axis.com/dam/public/74/23/8f/datasheet-axis-p1435-le-network-camera--en-US-270676.pdf>.
- [24] AXIS COMMUNICATIONS. *AXIS P3225-LVE Mk II Network Camera: Streamlined, outdoor-ready HDTV 1080p fixed dome for any light conditions*. Online. 2017. Dostupné také z: <https://www.axis.com/dam/public/d4/b3/8f/for-thailand-ict-specification-for-axis-p3225-lve-mk-ii-network-camera-en-US-108368.pdf>.
- [25] AXIS COMMUNICATIONS. *AXIS Q3505-V Network Camera: HDTV at 60 fps and top-of-the-line video quality*. Online. 2015. Dostupné také z: <https://www.axis.com/dam/public/29/61/f2/axis-q3505-v-network-camera-en-US-206263.pdf>.
- [26] COMMSYS TECHNOLOGY. *POPLACHOVÉ ZABEZPEČOVACÍ A TÍSŇOVÉ SYSTÉMY (PZTS)*. Online. Commsys Technology. Dostupné z: <https://commsys.cz/bezpecnostni-technologie/poplachove-zabezpecovaci-a-tisnove-systemy-pzts/>. [cit. 2025-05-27].

- [27] ČESKÁ AGENTURA PRO STANDARDIZACI. ČSN EN 50131-1 ed. 2, *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. Praha: Český normalizační institut, 2007.
- [28] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. 2006. ISBN 80-902938-2-4.
- [29] VELAS, Andrej. *ELEKTRICKÉ ZABEZPEČOVACIE SYSTÉMY*. Online, Skriptá. Žilina: ŽILINSKÁ UNIVERZITA V ŽILINE, 2010. Dostupné z: <https://www.researchgate.net/publication/337732617>. [cit. 2025-05-31].
- [30] MINISTERSTVO VNITRA. *Metodika výpočtu TCO ICT služeb veřejné správy*. Online. Architektura eGovernmentu ČR. 2022. Dostupné z: https://archi.gov.cz/znalostni_baze:metodika_tco. [cit. 2025-05-27].

ZOZNAM OBRÁZKOV

Obrázok 1 Bloková schéma kamery	37
Obrázok 2 Princíp CMOS snímača.....	38
Obrázok 3 Princíp CCD snímača.....	39
Obrázok 4 Princíp funkcie magnetického kontaktu.....	54
Obrázok 5 Schéma elektrického pripojenia magnetických kontaktov.....	55
Obrázok 6 Elektrické pripojenie čidiel na ochranu sklenených plôch.....	56
Obrázok 7 Spôsob umiestnenia kontaktných snímačov	58
Obrázok 8 Spôsob umiestnenia piezoelektrického snímača	59
Obrázok 9 Akustický detektor rozbitia skla	60
Obrázok 10 Konštrukcia PIR detektora	62
Obrázok 11 Zóny PIR detektoru	63
Obrázok 12 Lom IR žiarenia vo Fresnelovej šošovke	64
Obrázok 13 Charakteristika kombinovaného čidla.....	67
Obrázok 14 Aplikácia závesových čidiel.....	69
Obrázok 15 Konštrukcia mikrofonickeho kábla	71
Obrázok 16 Prekrytie infračervených lúčov	72
Obrázok 17 Kamera smerujúca na vnútorné priestory laboratória	88
Obrázok 18 Kamera smerujúca na vonkajšie prostredie	89
Obrázok 19 Kamera snímajúca prechodové podmienky (zhasnuté svetlo).....	90
Obrázok 20 Kamera snímajúca prechodové podmienky (zapnuté svetlo)	90
Obrázok 21 Zapojenie merača, switchu a kamery	92
Obrázok 22 Zabezpečovacia ústredňa so zapojenými periférnymi zariadeniami.....	109

ZOZNAM TABULIEK

Tabuľka 1 Rozdiel medzi LCC a TCO	20
Tabuľka 2 Technické parametre kamery AXIS M1045-LW	44
Tabuľka 3 Legenda skratiek z tabuľky 2	45
Tabuľka 4 Technické parametre kamery AXIS Q1635	46
Tabuľka 5 Legenda skratiek z Tabuľky 4	47
Tabuľka 6 Technické parametre kamery AXIS P1435-LE.....	48
Tabuľka 7 Legenda skratiek z Tabuľky 6	49
Tabuľka 8 Technické parametre kamery AXIS P3225-LVE Mk II	50
Tabuľka 9 Legenda skratiek z Tabuľky 8	50
Tabuľka 10 Technické parametre kamery AXIS Q3505-V	51
Tabuľka 11 Faktory TCO pre VSS a PZTS podľa fáz životného cyklu a nákladových kategórií	76
Tabuľka 12 Kategória nákladov podľa TCO	78
Tabuľka 13 Spotreba elektrickej energie	94
Tabuľka 14 Porovnania kamier podľa dátovej náročnosti.....	96
Tabuľka 15 Denný a mesačný objem dát na kameru	97
Tabuľka 16 Porovnanie nákladov kamier	100
Tabuľka 17 Porovnanie kamier podľa náročnosti.....	103
Tabuľka 18 Porovnanie ročných nákladov kamier	105
Tabuľka 19 TCO kamier.....	107
Tabuľka 20 Spotreba ústredne a periférií.....	110
Tabuľka 21 Náklady na elektrickú energiu ústredne a jej periférií	110

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

TCO	Total Cost of Ownership
IT	Informačné Technológie
LCC	Life Cycle Cost
SaaS	Software as a Service
AI	Artificial Intelligence
PTV	Priemyselná TeleVízia
CCTV	Closed Circuit TeleVision
VSS	Video Surveillance System
IP	Internetový Protokol
DVR	Digital Video Recorder
HDMI	High-Definition Multimedia Interface
HD	High Definition
USB	Universal Serial Bus
PoE	Power over Ethernet
PTZ	Pan-Tilt-Zoom
Wi-Fi	Wireless Fidelity
CMOS	Complementary Metal-Oxide Semiconductor
CCD	Charge-Coupled Device
A/D	Analog/Digital
RGB	Red-Green-Blue
NVR	Network Video Recorder
IoT	Internet of Things---
IR	Infra Red
LED	Light-Emitting Diode
LAN	Local Area Network

FPS	Frames Per Second
px	PiXel
MJPEG	Motion Joint Photographic Experts Group
SD	Secure Digital
SDHC	Secure Digital High Capacity
NAS	Network Attached Storage
GHz	GigaHertz
W	Watt
RH	Relative Humidity
mm	MiliMeter
g	Gram
Č/B	Čierno/Biela
dB	deciBel
IEEE	Institute of Electrical and Electronics Engineers
af	AutoFocus
V	Volt
DC	Direct Current
AES	Advanced Encryption Standard
°C	Stupeň Celzia
kg	KiloGram
HFOV	Horizontal Field Of View
NEMA	National Electrical Manufacturers Association
IK	Impact protection rating (IK code)
VMD	Video Motion Detection
SDXC	Secure Digital eXtended Capacity
WDR	Wide Dynamic Range

EZS	Elektrická Zabezpečovací Signalizácia
PCO	Pult Centralizovanej Ochrany
PIR	Passive InfraRed
US	UltraSonic
MW	MicroWave
SIM	Subscriber Identity Module
NAS	Network Attached Storage
HDD	Hard Disk Drive
DPH	Daň Pridanej Hodnoty
RFID	Radio-Frequency Identification