Moderní technologie v zajištění bezpečnosti pláště budov

Modern technologies ensure the security of building shell

Roman Kudlička

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Roman KUDLIČKA**
Osobní číslo:	**A08352**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Moderní technologie v zajištění bezpečnosti pláště budov**

Zásady pro vypracování:

1. **Zpracujte manuál pro managery průmyslu komerční bezpečnosti k zabezpečení produktu "dodávka a montáž technologií k zajištění bezpečnosti pláště budov".**
2. **Charakterizujte problém v zabezpečení pláště budov s přihlédnutím k trestné činnosti krádeží vloupáním.**
3. **Uveďte takticko-technické řešení problému.**
4. **Uveďte vhodnost materiálů na trhu v České republice a Evropské unii.**
5. **Popište certifikaci a zkušebnictví v oboru.**
6. **Uveďte vývojové trendy a prognózu směru vývoje.**
7. **Proveďte konkrétní návrh pro zvolený objekt.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 3. aktualiz. S.l. : Cricetus, 2006. 313 s. ISBN 80-902938-2-4(brož.)**
2. **KINDL, Jiří. Projektování bezpečnostních systémů I. 2. vyd. Zlín : Univerzita Tomáše Bati, 2007. 134 s. ISBN 978-80-7318-554-1.**
3. **ZEMAN, Petr. Česká bezpečnostní terminologie. Brno : Masarykova univerzita , 2002. 186 s. ISBN 80-210-3037-2.**
4. **IVANKA, Ján. Systemizace bezpečnostního průmyslu I. 3. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 123 s. ISBN 978-80-7318-850-4.**
5. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 3. Zlín : Univerzita Tomáše Bati ve Zlíně, 2010. 81 s. ISBN 978-80-7318-889-4.**
6. **ČANDÍK, Marek. Technické prostředky bezpečnostního průmyslu. Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta technologická, Ústav elektrotechniky a měření, 2005. 117 s. ISBN 8073183285.**

Vedoucí bakalářské práce: **JUDr. Vladimír Laucký**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ Fakulta aplikované informatiky L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Cílem této bakalářské práce je zpracovat orientační manuál pro manažery PKB z hlediska zajištění bezpečnosti pláště budov obsahující dodávku a montáž technologií. V první kapitole se budu věnovat problematice zabezpečení pláště budov s přihlédnutím k trestné činnosti krádeží vloupáním se do objektu, zde uvedu a rozeberu statistiku způsobů vloupání do objektů. V následující kapitole se budu věnovat takticko-technickému řešení, uvedu používané technické prvky zajišťující bezpečnost pláště objektu, jejich princip činnosti, základní parametry a zásady montáže. Další kapitola bude pojednávat o dostupném materiálu na trhu ČR a EU z hlediska výrobců a distributorů. Následující kapitola bude zaměřena na legislativu certifikace a zkušebnictví dle českých zákonů, nařízení vlády a normativních úprav. Závěrečnou kapitolu teoretické části věnuji vývojovým trendům a prognóze směru vývoje technického zabezpečení objektů. Praktická část bakalářské práce pak bude obsahovat návrh zabezpečení pro konkrétní objekt.

Klíčová slova: bezpečnost, objekt, vloupání, detektory, přístupový systém, biometrie, certifikace, zkušebnictví, trendy, návrh zabezpečení

ABSTRACT

Objective of this thesis is to elaborate guide manual for managers of commercial security in terms of ensuring the security shell of buildings that contain delivery and installation technologies. The first chapter will be devoted to security issues to building shell regard the crime theft by break into building, and I will discuss statistics of breaking into buildings. The next chapter will be devoted to tactical and technical solutions, I will describe used technical features to ensure security of the building shell, their working principle, the basic parameters and principles of the installation. The next chapter will discuss the available equipment on the market of Czech Republic and European Union in terms of manufacturers and distributors. The next chapter will focus on legislation and certification testing according to Czech law, government order and regulatory regime. The final chapter of this section is devoted to development trends and forecast the direction of the development of technical security of facilities. Practical part will contain a security design for a specific object.

Keywords: security, facility, breaking in, detectors, access control system, biometrics, certification, testing, trends, security design

Tímto bych rád poděkoval vedoucímu mé bakalářské práce panu JUDr. Vladimíru Lauckému za vedení a poskytování připomínek a námětů při tvorbě bakalářské práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že 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;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona 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);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že 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 samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Zajištění bezpečnosti pláště objektů je důležité z hlediska stavu bezpečnosti uvnitř objektu, ať už se jedná o ochranu majetku či zdraví a života osob uvnitř. Tuto bezpečnost obvykle zajišťují tři na sobě závislé a nepostradatelné složky skládající se z ochrany fyzické, režimové a technické, ve své práci se věnuji poslední z těchto složek a to ochraně technické.

Tuto problematiku lze rozdělit na dva způsoby vniknutí do objektu/narušení bezpečnosti pláště a to na násilný způsob a způsob nenásilný. Mezi násilné způsoby lze zařadit pokus o průstup skrze okna rozbitím skla či vypáčením, roztažení mříží, vyražením dveří apod. či ještě radikálnější a to proražení skrz zeď či střechu objektu. Do nenásilných pokusů pak spadají pokusy o neoprávněný průnik do objektů s pomocí zcizených či zfalšovaných přístupových předmětů, jako jsou klíče, čipové karty či hesla. Před tímto způsobem vniknutí do objektu chrání moderní přístupové systémy např. biometrické snímající jedinečnou biometrii osob na základě daktyloskopických metod, geometrie ruky, oční duhovky, sítnice a dalších či kamerové systémy, které se mohou též řídit biometrií obličejů snímaných kamerou.

Důležitým prvkem při ochraně pláště objektu je také ochrana perimetru před pohybem nepověřených osob, proto jsou obsahem mé práce i detektory perimetrické, nejen typické plášťové. Pokud je totiž potencionálnímu pachateli umožněn přístup do blízkosti napadnutelného objektu, je již jen omezená možnost útoku zabránit, cílem tedy je detekovat útočníka dříve, než dojde k samotnému narušení pláště objektu a eliminovat případnou hrozbu.

Dle oficiálních dokumentů Policie České republiky lze vysledovat neustálý nárůst počtu krádeží vloupáním a obecně majetkové trestné činnosti, při níž dochází ke stále se zvyšujícím finančním ztrátám, z tohoto důvodu narůstá i počet soukromých bezpečnostních služeb.

I. TEORETICKÁ ČÁST

1 ZABEZPEČENÍ PLÁŠTĚ

1.1 Základní bezpečnostní terminologie

Základem v bezpečnostním sektoru je volit správné významové termíny z důvodu správného pochopení situace a zamezení zmatků a nepřesností. To byl v minulosti problém, protože přístup k utváření termínů byl multidisciplinární povahy, v praxi prováděn více obory, mezi nimi např. zabezpečení informačních systémů a komunikací, krizové řízení, politologie, vojenská teorie, technické obory. Ty samostatně vznikaly a také se téměř samostatně vyvíjely.

Obecně platí pro terminologie každé odborné disciplíny tyto důležité vlastnosti:

- Ustálenost – zaručující bezporuchovost komunikace
- Systémovost – zajišťující sepětí termínů daného oboru
- Přesnost a jednoznačnost – i ve vztahu k synonymům a ostatním oborům
- Nosnost – schopnost být východiskem při tvorbě nových termínů

Postupem času se stala terminologická nepřesnost zjevnou a nezanedbatelnou, bylo potřeba ji sjednotit, včetně základních nejobecnějších běžně intuitivně používaných termínů (bezpečnost, hrozba, riziko,…), které často vedly k nedorozumění, i přesto je intuitivní chápání do jisté míry nepostradatelné. Tato nepřesnost nebyla zapříčiněna pouze specializací jednotlivých oborů, ale také překlady z/do ostatních jazyků, jež jsou někdy problematické. Příkladem bylo NATO Glossary of Terms and Definitions vydávaný NATO Standartization Agency pravidelně renovovaný, další vymezování pojmů bylo prováděno pomocí platných zákonných norem.

Za účasti Ústavu strategických studií Vojenské akademie v Brně a spolupráci s Ústavem mezinárodních vztahů v Praze byl svolán seminář, na němž bylo konstatováno, že základní pojmy bezpečnostní terminologie jsou užívány nejednotně i v oficiálních dokumentech ČR a byl přijat návrh na sestavení pracovní skupiny skládající se z odborníků jednotlivých oborů, aby zpracovala studii a návrh definicí.

1.1.1 Bezpečnost

Výraz bezpečnost je důležitý základní pojem v bezpečnostním průmyslu, je využíván v mnoha odvětvích od společenskovědních oborů (politologie, ekonomie, sociologie,…) přes přírodovědní obory (medicína, ekologie) po technické (informatika, strojírenství, elektrotechnika).

Dle Slovníku spisovné češtiny pro školu a veřejnost je pro přídavné jméno bezpečný uváděno jako synonymum jistý. V bezpečí je tedy člověk, jež není vystaven žádnému nebezpečí, nebo je před nebezpečím chráněn.

Problém avšak vyvstává při překladu z/do angličtiny, kde jsou má výraz bezpečnost dva významy a to safety a security, ve slovnících nejsou rozlišovány a znamenají totéž, i když ve skutečnosti totéž neznamenají. Pojem **safety** skýtá bezpečnost ve vazbě na jednotlivce, v obecném významu (politologie) je užíváno výrazu **security**.

1.1.2 Hrozba a riziko

Pojmy hrozba a riziko patří po boku bezpečnosti též mezi klíčové základní pojmy v bezpečnostním sektoru. Jsou běžně využívány v hovorech, publikacích a odborných literaturách všech možných oborů, ale nikde nejsou konkrétně definovány, ani v NATO.

Obecný význam

Oba výrazy jsou běžně lidmi navzájem zaměňovány, v jazykovědných a encyklopedických slovnících jsou definovány jen s drobnými rozdíly.

Hrozba – slovo domácího původu, má významy: blížící se nebezpečí, hrožení, výhružka, nátlak.

Riziko – pochází z italského risico, významy balancují mezi dvěma variantami: nebezpečí nezdaru, zranění, škody, ztráty a hazard, možnost vzniku nežádoucí situace.

Bezpečnostní a odborné dokumenty

V tomto sektoru bylo užívání výrazů hrozba a riziko nejvíce rozkolísané, často zaměňováno a nesprávně užíváno, dokonce i v zákonech ČR, a zčásti je tomu tak i dnes. Největší nestálost těchto výrazů trvala do roku 1999 do publikací Úřadu pro zahraniční styky a informace (později i dalších institucí), kde byly oba tyto termíny přesně a podrobně definovány

Správné užití

Hrozba je vnější činitel, který může nebo chce způsobit škodu konkrétní hodnoty, závažnost je přímo úměrná povaze a ceně hodnoty. Může být neintencionální tedy jevem přírodní povahy, nebo intencionální čili působená či zamýšlená s úmyslem.

Riziko znamená pravděpodobnost škody/ztráty, tedy vyjadřuje pravděpodobnost možnosti nastání nežádoucí situace. Za jistých okolností může být klasifikovatelné vyjádřeno procenty či podíly nebo alespoň klasifikovatelné do tříd. Riziko jako takové je závisle proměnnou, dá se určit nebo odhadnout analýzou rizik, je reakcí na hrozbu.

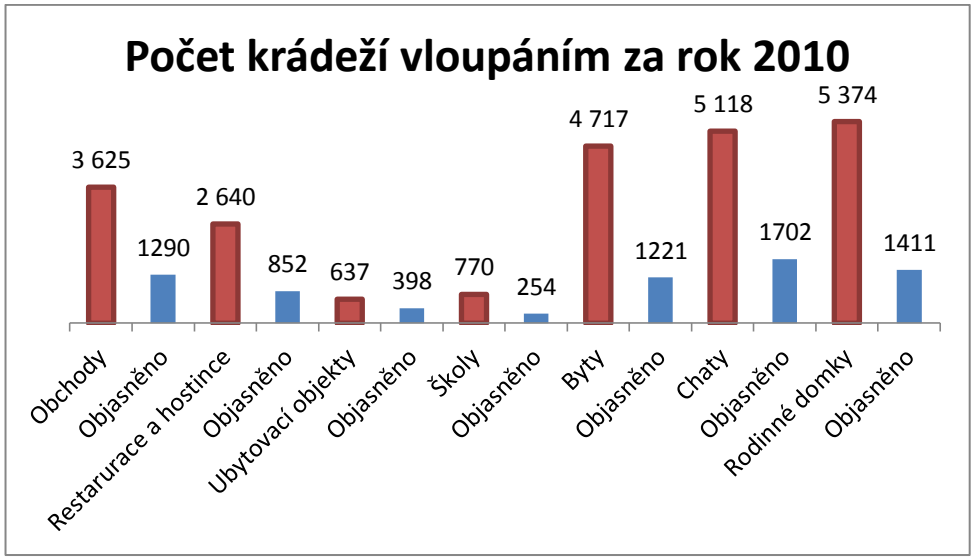
1.1.3 Objekt a objektová ochrana

Objekt je budova nebo jinak stavebně vymezený prostor, ve kterém se nachází chráněné cenné hodnoty.

Objektová ochrana je bezpečnostní proces, který poskytuje chráněnému objektu technickou, taktickou a personální ochranu před hrozbami tak, aby byl objekt co nejvíce bezpečný před rizikem a byla eliminována nebo alespoň minimalizována pravděpodobnost narušení, poškození či zcizení.

1.2 Trestná činnost vloupání v ČR

Trestnou činností vloupáním se zabývá Policie České republiky (PČR), vycházím z jejich prezentovaných statistických údajů zveřejňovaných na stránkách Policie České republiky. Dle těchto dat bylo v roce 2010 zaznamenáno 58 758 krádeží vloupáním, při nichž došlo k majetkovým ztrátám ve výši 2 331 750 000 Kč. Z těchto krádeží vloupáním bylo objasněno či objasněno dodatečně celkem 13 708 případů a navráceno majetku v hodnotě 33 297 000 Kč. V procentuálním vyjádření jde o 23,33% objasněnost případů a 1,43% navráceného majetku. Za tuto trestnou činnost bylo zodpovědných 9114 osob, z toho 5418 byli recidivisté! Vyjádřeno v grafu.



Graf 1: Počet krádeží vloupáním za rok 2010 [9]

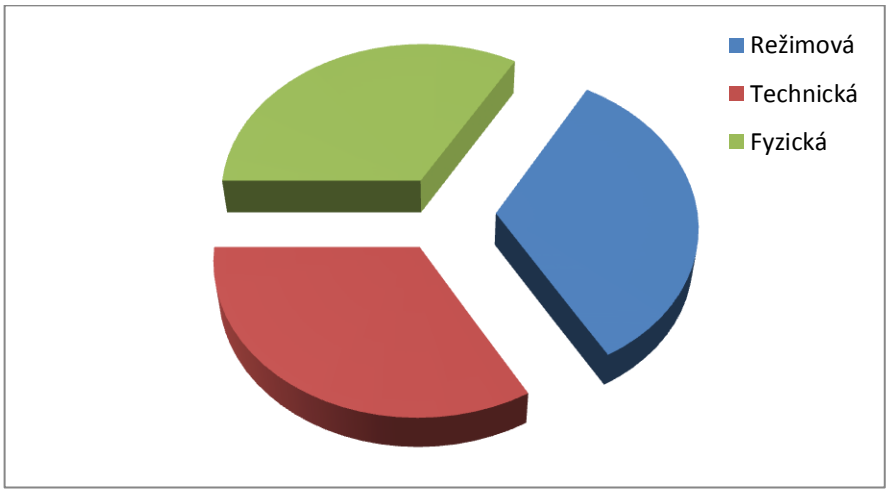
Graf 2: Škody způsobené krádežemi vloupáním za rok 2010 [9]

Z údajů a grafů je jasně patrný nepoměr mezi vyřešenými případy a zajištěným majetkem, drtivá většina zcizeného majetku zůstane nezajištěna. Více než 80% trestné činnosti připadá kriminalitě majetkové, která se koncentruje zejména ve velkých městech a průmyslových aglomeracích s vysokým počtem osob. Pokud tedy člověk v takové oblasti žije a myslí si, že se jej to netýká a nemůže se mu to stát, jde o velký omyl. Z údajů vyplývá, že v roce 2010 bylo v průměru vykradeno 14,72 rodinných domků, 12,92 bytů a 9,93 obchodů každý den.

1.3 Objektová ochrana

Cílem objektové ochrany je navrhnout takový bezpečnostní systém, aby byla opravdu zajištěna bezpečnost objektu. Za tímto účelem je třeba znát dvě základní věci a to **předmět ochrany** (co je chráněno) a **cíl ochrany** (jaká je reálná hrozba).

Každý komplexní bezpečností systém by se měl skládat z ochrany technické, fyzické a režimové.



Graf 3: Ochrana objektu

Technická ochrana

Technickou ochranu lze rozdělit na dvě složky a to na MZS (mechanický zábranný systém) a PZS (poplachový zabezpečovací systém).

MZS chrání objekt svou mechanickou odolností, ta je často klíčová při napadení objektu útočníkem, určuje to, jakou dobu bude schopna útočníkovi odolávat, na to má vliv bezpečnostní třída MZS a vybavenost útočníka. Sem patří ploty, brány, závory, mříže, rolety, bezpečnostní polepy, fólie, skla, kování, zámky, trezory atd.

Obr. 1 Pyramida bezpečnosti [30]

PZS zpravidla neznemožňuje pachateli vloupat se do objektu, pouze upozorňuje na jeho přítomnost, rozšiřuje tak vnímací schopnosti fyzické ochrany, která při zjištění útok provede zásah. Spadají sem PZS, ACS, EPS, CCTV atd.

Fyzická ochrana

Je jedním z klíčových prvků ochrany, zasahuje při zjištění přítomnosti útočníka, jde o živou sílu, závisí na ní výsledná bezpečnost systému. Dále se dělí na statickou, která hlídá u vchodů a dynamickou, která hlídkuje ve vymezeném prostoru.

Režimová ochrana

U režimové ochrany jde výhradně o soubor organizačně administrativních opatření a postupy směřující k zajištění požadovaných podmínek. Dělí se na vnější, kde jde zejména o vstupní a výstupní politiku chráněného prostoru a vnitřní, kde jde o omezení pohybu osob dle oprávnění.

Z hlediska chráněného prostoru se technická ochrana člení na:

Perimetrická ochrana

Rozkládá se po obvodu chráněného objektu, tím je obvykle myšlena katastrální hranice obvykle tvořená bariérami (umělými či živými ploty, zdí,…). Často bývá podceňována, je to první vrstva bezpečnostního systému, může být z hlediska bezpečnosti klíčová, čím dříve pachatele zaznamenáme/odradíme, tím lépe pro bezpečnost samotného chráněného objektu.

Plášťová ochrana

Je druhou vrstvou bezpečnostního systému, signalizuje narušení pláště střeženého objektu, obvykle je realizována vnitřně. Zpravidla jde o detektory tříštění skla, otřesové, magnetické kontakty atd.

Prostorová ochrana

Střeží samotný interiér chráněného objektu, detekuje změny vyvolané útočníkem, který již vnikl do vnitřních prostor. Nejčastěji jde o PIR, MW, US a duální detektory, které snižují možnost falešných poplachů.

Předmětová ochrana

Chrání již jednotlivé chráněné předměty ve střeženém prostoru, signalizuje jejich napadení či neoprávněnou manipulaci s nimi. Otřesové detektory, detektory na ochranu zavěšených předmětů, kapacitní detektory.

Tísňová ochrana

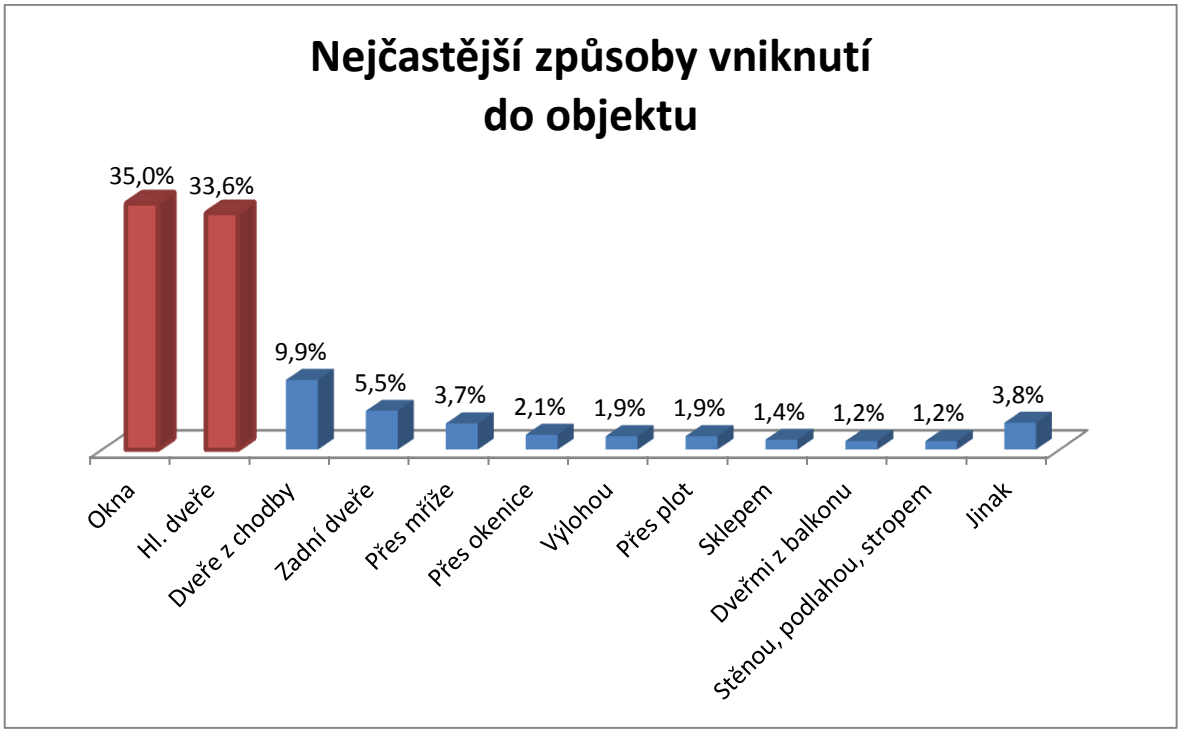
Signalizuje ohrožení osoby napadením nebo živly, tlačítka, klíčenka apod.

Tab. 1 Stupně zabezpečení dle ČSN EN 50 131-1 ed. 2

Stupeň	Název stupně	Předpokládaná výbava narušitele
1	nízké riziko	Narušitel má malou znalost PZTS, omezený sortiment snadno dostupných nástrojů.
2	nízké až střední riziko	Narušitel má omezené znalosti PZTS, běžné nářadí a přenosné přístroje.
3	střední až vysoké riziko	Narušitel je obeznámen s PZTS, rozsáhlý sortiment přístrojů a přenosných elektronických zařízení.
4	vysoké riziko	Narušitel je schopen, nebo má možnost zpracovat podrobný plán vniknutí a má kompletní sortiment nářadí.

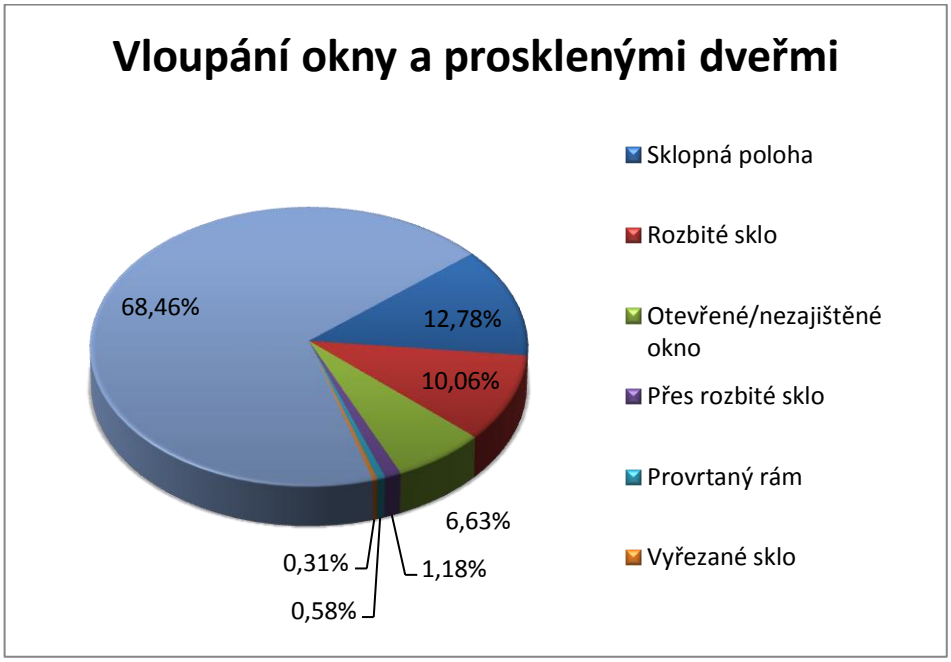
1.4 Způsoby vniknutí do objektu

Pachatelé pro vloupání se do objektu nejčastěji zpravidla volí ten nejsnazší a tedy nejnáchylnější způsob a tím jsou průstupové otvory okna a dveře, přes jiné komplikovanější mechanické zábranné systémy se rozhodují daleko méně často. Proto je důležité náležitě zabezpečit i tyto nejnáchylnější části objektu, zabezpečení objektu jako celku je tak silné jako jeho nejslabší článek, je tedy zbytečné investovat do masivních bezpečnostních vchodových dveří za velký peníz a nechat pak útočníkovi prakticky téměř volnou cestu obyčejnými nechráněnými okny.



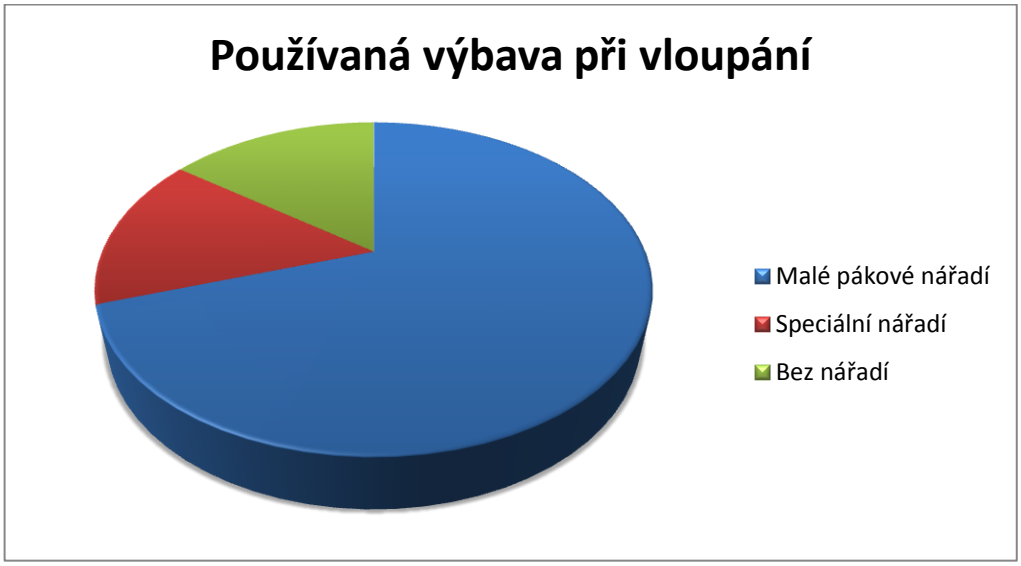
Graf 4: Nejčastější způsoby vniknutí do objektu [30]

Z následujícího grafu je jasně patrné, že se útočníci málokdy pouštějí skrze prosklenou výplň oken a dveří a to z důvodu vysoké hlučnosti, která by přilákala pozornost okolí. Nejčastěji tak útočí na samotný okenní rám, k samotnému takovému útoku útočníkovi postačí i menši snadno dostupné nářadí jako šroubováky apod.



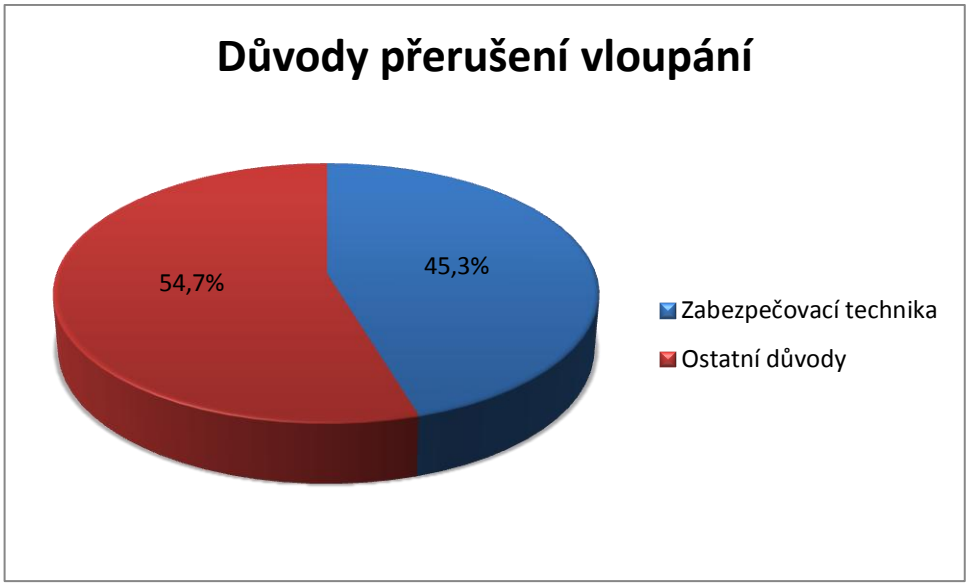
Graf 4: Nejčastější způsoby vniknutí do objektu [31]

Používaná výbava pachateli bývá z větší části malá snadno dostupná a přenosná, jen malá část pachatelů využívá hůře dostupných speciálních vybavení, zhruba stejná část pachatelů se rozhodne k vloupání do objektu bez nářadí pouze hrubou silou.



Graf 4: Nejčastější způsoby vniknutí do objektu [31]

Aby chráněný objekt odolal útoku útočníka, musí být zabezpečovací systém schopný odolávat útoku útočníka po určitou kritickou dobu tak, aby byla snaha útočníka překonána anebo byl jeho pokus zastaven jiným zásahem.



Graf 4: Nejčastější způsoby vniknutí do objektu [32]

2 TAKTICKO-TECHNICKÉ ŘEŠENÍ

2.1 Kamerové systémy CCTV

Jsou nedílnou součástí zabezpečovacího systému především komerčních středně velkých a velkých objektů, umožňují střežit rozsáhlé okolí z jednoho či více míst obsluhou hlídající monitory za účelem identifikace osob a monitoringu jejich pohybu, odhalování a prevenci trestných činů, dohlížení na bezpečnost práce a technologických procesů. Zároveň může být snímaná scéna zaznamenávána do archivu, dnes nejčastěji na pevné disky o dostatečné kapacitě HDD v počítačích anebo digitálních rekordérech DVR. Dříve byly k této funkci využívány zejména analogové kamery, ty jsou dnes již na ústupu a přezbrojuje se na digitální IP kamery, které mají oproti starým analogovým daleko lepší rozlišovací schopnosti a další výhody.

2.1.1 Hlavní parametry kamer

Rozlišovací schopnosti

Rozlišení je základní parametr udávající, kolik je čip kamery schopen zaznamenat bodů, udává se zpravidla v TV řádcích. Analogové standardní rozlišení 400 řádků černobílého záznamu (EIA/CCIR), 330 řádků barevného (NTSC/PAL), používá se tam, kde netřeba snímat detaily např. celkový přehled. Vysoké rozlišení 570 až 710 černobílých řádků, 420 až 550 barevných řádků určené ke snímání detailů obličejů a následné zpracování. Digitální kamery v řádech MPx dle přenosového media.

Citlivost

Je udávána v jednotkách Lux, udává potřebné světelné podmínky pro fungování. Standardní u černobílých kamer 0,1 Lux, barevné 1 Lux, postačuje pro běžné světelné podmínky za denního světla či umělého osvětlení. Vysoká citlivost u černobílých kamer 0,001 Lux, barevné 0,01 Lux, tyto kamery jsou schopny snímat za sníženého osvětlení za přítomnosti minimálního osvětlení, černobílé jsou vždy nejméně o řád citlivější.

Snímání

Může být barevné či černobílé, lze kombinovat, za dostatečného osvětlení pracuje čip v barevném modu a za zhoršených světelných podmínek dojde k přepnutí do černobílého modu.

Přísvit

Zpravidla pomocí IR diody infračerveným světlem, slouží ke snazšímu snímání scény za zhoršených podmínek, vysoce efektivní, většinou u dražších kamerových systémů.

Obr. 2 Kamera s IR přísvitem [14]

Přenos

U moderních digitálních IP kamer probíhá digitálně, je možný i na velké vzdálenosti, lze použít opakovače (zesilovače) signálu.

Po nesymetrickém vedení – Koaxiál 50 Ohm, umožňuje přenos řádově do několik málo stovek metrů, nutné dovést do kamery napájení zvlášť

Po symetrickém vedení – Kroucená dvojlinka, spíše nestíněná UTP - levnější, delší dosah, STP stíněná. Umožňuje přenos i na několik km, má vyšší odolnost vůči rušení oproti koaxiálu, lze jím realizovat i napájení kamery.

Bezdrátově – Nejčastěji probíhá na dvou kmitočtových pásmech 2,4 a 10GHz, mají omezený výkon a tedy i dosah. Řídí se dle normy Českého telekomunikačního úřadu GL 14/R/2000.

Po optickém vlákně – Při přenosu dochází k minimálním ztrátám, praktické žádné interference. Vzdálenost přenosu možná i na desítky km, problémem je pouze instalace, nelze jej lámat.

Infračervený přenos – Má velice omezený rozsah, dosah i rychlost, lze se s ním setkat při přenosu snímků z detektorů.

Napájení

Možné způsoby ze sítě 230V AC, 12V DC, Ethernet PoE.

Ovládání

Například PTZ (Pan, Tilt, Zoom) - je schopno ovládat vzdáleně z ovládacího pultu či klávesnice pohyb kamery a to doleva, doprava, nahoru, dolu a přiblížení zoom.

2.1.2 Typy kamer dle účelu

Vnitřní kamery – Svou technickou konstrukcí jsou určeny pro použití ve vnitřních prostorách bez extrémních povětrnostních podmínek, tedy bez vlhkosti, prašnosti a velkých teplotních výkyvů.

Venkovní kamery – Svoji konstrukci mají přizpůsobenou pro funkci ve vnějších prostorech v náročnějším prostředí na povětrnostní vlivy.

Vodotěsné kamery – Jsou uzamknuty ve voděodolných krytech vhodné při potápění či do bazénů.

Dome kamery – Zpravidla v půlkruhovém krytu připevňované vodorovně na strop, obsahují systém PTZ, tedy lze s nimi otáčet a měnit zoom.

Obr. 3 Kamera v provedení dome [14]

Antivandal kamery – Zabudované do robustních krytů mechanicky odolných proti případnému útoku hrubou silou.

Atrapy kamer – Těžko rozeznatelné laikem na první pohled od skutečných kamer, slouží pro odstrašení případných pachatelů. Zpravidla bývá kombinována se skutečnými kamerami.

Obr. 4 Atrapa kamery [16]

2.1.3 Snímací prvek

Ve videotechnice jsou dva nejčastěji využívané prvky pro snímání obrazu a to CCD a CMOS.

CCD

Čip CCD je nejčastěji využívaným čipem ve videotechnice pro záznam obrazu. Výstupní informace z CCD čipu není digitální, ale analogová, a proto je třeba za něj umístit obvody převodníku A/D, které způsobují vyšší odběr elektrické energie.

Dále se čipy CCD rozdělují na progresivní a prokládaný. **CCD progresivní** mají řádky či sloupce světlo citlivých buněk napojeny na jednu sběrnici za účelem jednoduchosti a ceny, což má za následek pomalejší zpracování dat. Data jsou postupně zpracovávána po řádcích či sloupcích. **CCD prokládané** na rozdíl od CCD progresivního již nezpracovává po jednotlivých řadách či sloupcích, ale po blocích, každý z nich má vlastní registr, což je malé dočasné úložiště dat, které urychluje práci s nimi (nutné v případech, kde je nutno pořízení více snímků rychle za sebou).

CMOS

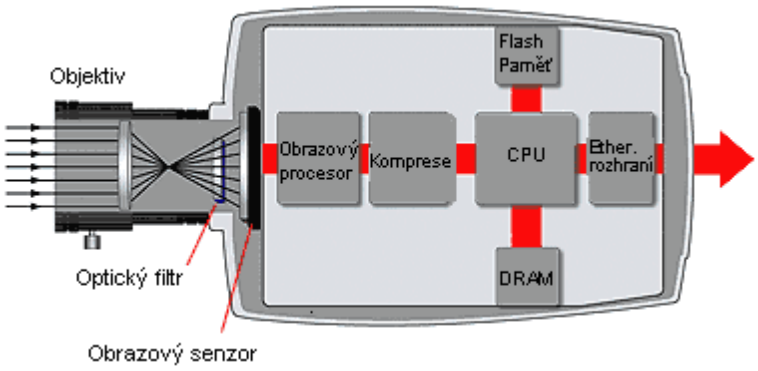
CMOS čip je oproti CCD výrobně méně nákladný a to z důvodu stejné výrobní technologie jako počítačové procesory. Digitalizace každého obrazového bodu je prováděna samostatně a to tak, že digitalizační obvody jsou přímo součástí každého CMOS čipu, digitalizace tak probíhá téměř okamžitě a u všech zaráz, to snižuje dobu potřebnou pro pořízení snímku a také spotřebu elektrické energie zařízení. Co se týká konstrukce CMOS, tak světlo citlivé prvky zabírají pouze nepatrnou část celého čipu, zbytek jsou digitalizační obvody, proto je před každý světlo citlivý prvek mimo RGB filtru umístěna čočka soustředící světlo do jednoho malého bodu.

2.1.4 IP kamery

V současnosti nejvíce užívané kamery v bezpečnostním průmyslu díky svým technickým možnostem, jsou též nazývány jako webové kamery, ty ke své funkci oproti webkamerám nepotřebují PC, veškeré nutné prostředky má integrovány v sobě. Připojuje se zpravidla klasickou nestíněnou kroucenou dvojlinkou UTP se zakončením RJ-45, kterým je realizováno i napájení, a dostupná může být buď jen v rámci objektu LAN, nebo v celé síti Internet. Každá IP kamera má vlastní IP adresu, na kterou se lze připojit, na dané IP adrese se nachází webové prostředí IP kamery, které může mít zabezpečený přístup na heslo. V tomto webovém prostředí lze provádět veškerá nastavení kamery, jako jsou

rozlišovací schopnosti, citlivost, zóny detekce pohybu atd. Možnosti nastavení detekce pohybu jsou odvislé od výrobce a cenové relace, v těch lepších lze nastavit i směr pohybu pro vyvolání poplachu, u PTZ IP kamer i automatizované natáčení kamer (tzv. auto-tracking) za pohybujícím se objektem, který vstoupil do zóny. Kromě webového serveru obsahuje též FTP klient a server a emailového klienta, přes které lze zasílat zprávy včetně pořízených jednotlivých snímků, a dalších mnoho funkcí jako programovatelné vstupy a výstupy a další.

Hlavním omezením použití IP kamer dnes jsou kapacity přenosových cest, které nejsou zpravidla jen pro IP kamery samotné, ale k propojení dalších zařízení. Proto je nutné vhodně navrhnout typ, počty, umístění a konfiguraci kamer, aby nedošlo k zahlcování sítí.



Obr. 5 Blokové schéma IP kamery [33]

2.1.4.1 Způsob záznamu

Možnosti záznamu z IP kamer se dělí na softwarové řešení, řešení za použití PC s příslušným interface a hardwarové řešení.

Softwarové řešení

Za použití softwarového řešení není třeba žádného specializovaného zařízení ani softwaru, stačí pouze zadání IP adresy požadované IP kamery do adresního pole internetového prohlížeče, kterým disponuje každý osobní počítač, případně ještě zadání přístupových autentizačních údajů. Z tohoto prostředí už může uživatel sledovat aktuální záběry

z kamery, ale nelze je ukládat jako video, většinou lze takto zachytit pouze ručně jednotlivé aktuální snímky. Lze se ale tímto způsobem připojit na disk kamery, videoserver či jiné záznamové zařízení, kde dochází k záznamu a záznamy z kamer přehrávat.

PC s interface

Toto řešení je realizováno samostatnou kartou připojovanou do osobního počítače, počet zaznamenávaných IP kamer je omezen hardwarovou vybaveností této karty, a specializovaným SW (může umožňovat i funkci server/klient). Limitujícím prvkem je i HW konfigurace počítače, zpracovávání videa klade vysoké nároky na výpočetní výkon.

Hardwarové řešení

Jedná se o specializované zařízení přizpůsobené pro záznam CCTV odborně nazývané NVR určené do náročných aplikací, ke své obsluze používá standardní počítačové periferie. Videozáznam ukládá na interní disky, které mají v současné době kapacity až v řádech TB, díky kterému je možno uložit velké množství videozáznamů, záleží však na počtu kamer a jejich rozlišovacích schopnostech popř. nastavené kompresi.

SW vybavení je volitelné od několika výrobců a liší se svými schopnostmi, zpravidla umí sledovat více kamer, ovládat PTZ, dále detekovat pohyb v obraze, alarmy, záznamy událostí, funkce server/klient a další.

2.2 Detektory tříštění skla

Detektory tříštění skla slouží jako plášťová ochrana k ochraně prosklených ploch, známy jsou též pod názvem glassbreak. Jsou navrženy tak, aby byl vyvolán poplach již při první nevratné změně skla např. proražení otvoru a odeslán na ústřednu PZS. Prakticky jsou to moderní nástupci poplachových fólií, polepů, tapet a skel, jejichž instalace je náročná. Mechanické vlivy jako otřesy, škrábání apod. nevedou ke spuštění alarmu.

Dle parametrů se liší hlavně svým fyzikálním principem, dosahem, spotřebou, detekční charakteristikou, určeným druhem skla, stupněm zabezpečení, stupněm utajení a cenou.

Dělí se do 3 skupin:

- Pasivní kontaktní
- Pasivní bezkontaktní
- Aktivní kontaktní

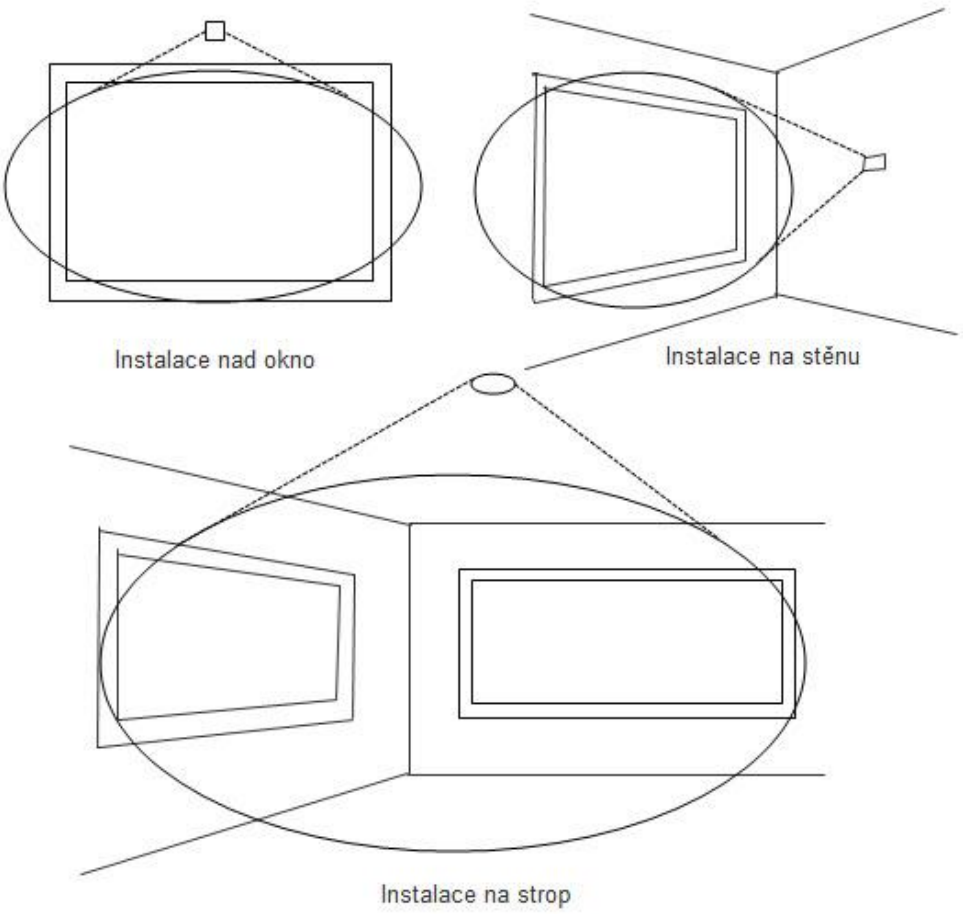
2.2.1 Pasivní kontaktní

Jsou fyzicky spojeny s prosklenou plochou, pracují na principu snímání rezonančního kmitočtu obvykle v pásmu 40 až 120kHz charakteristickém pro řezání a praskání skla s pomocí piezoelektrického krystalu, který při deformaci indukuje elektrické napětí. Ze zmíněných typů jsou schopny detekovat nejmenší plochu, umisťují se kvůli co nejmenšímu útlumu speciálním dvousložkovým lepidlem cca 5cm od rámu okna. Jsou tak snadno viditelná, což může útočníka zastrašit nebo vyzvat k jinému způsobu vloupání. Mají další řadu nevýhod, jako je ovlivnění funkce za nízkých venkovních teplot, kdy dochází k orosení skla, proto je lepší instalace v horních částech oken. Přesto jsou dnes spíše na ústupu a jsou nahrazovány lepšími technologiemi.

2.2.2 Pasivní bezkontaktní

Na rozdíl od kontaktních již nejsou fyzicky spojeny s chráněnou skleněnou plochou, ale snímá následný akustický efekt při tříštění skla na dálku šířený vzduchem. Elektronika vyhodnocuje akustické vlnění přijaté z prostoru pomocí piezoelektrického či elektretového mikrofonu, které je dále odfiltrováno pomocí pásmových propustí. Moderní pasivní bezkontaktní detektory tříštění skla využívají vícepásmových propustí, které vyhodnocují tříštění skla dle jednotlivých fází tříštění, tedy proražení a následný dopad. Tím jsou eliminovány falešné poplachy vyvolány vlivem prostředí např. kontejnery skla poblíž, doprava aj.

Charakteristika rozsahu už je lepší cca $15m^2$, umisťují se tak, aby na skleněné plochy bylo vidět, to umožní pokrytí více prosklených ploch, dále mezi detektorem a skleněnou plochou nesmí být závěsy, žaluzie atp., které snižují či zcela eliminují efektivnost detekce, typ detektoru musí být navrhnut na konkrétní typ skla. Bezpečnostní a jiné fólie snižují efektivnost v řádech desítek procent, mohou ale změnit charakteristiku tříštění tak, že detektor vůbec nezareaguje.



Obr. 6 Umístění pasivního bezkontaktního detektoru tříštění skla

2.2.3 Aktivní kontaktní

Oproti předchozím pasivním typům nesnímá pouze samotné prostředí, ale vytváří si své vlastní pracovní prostředí, ve kterém detekuje změnu oproti normálu. Jsou využívány v prostředí s nejvyšším rizikem, jsou nejspolehlivější a mají nejnižší četnost falešných poplachů. Skládají se ze dvou částí a to vysílače a přijímače, ty jsou opět připevněny na sklo s pomocí speciálního dvousložkového lepidla. Vysílací část obsahuje ultrazvukový generátor vysílající do skla signál a přijímací část umístěná na opačné straně rámu skla přijímá a vyhodnocuje. Mají velkou detekční plochu cca 25m^2, dle typu detektoru a skla.

Existuje i optický systém využívající IR světla, funkce je obdobná, při narušení skleněné plochy dojde ke změně charakteristiky přijímaného IR světla a tak dojde k vyvolání poplachu.

2.3 Štěrbinové kabely

Spadají do kategorie venkovní perimetrické ochrany, lze je označit za detektor aktivní, vytváří si své vlastní pracovní prostředí doutníkového tvaru, vf energie elektromagnetického charakteru, a detekují změnu jeho homogenity. Při vstoupení osoby či jiného pohybujícího se objektu do zóny dojde k poklesu amplitudy a tím k vyvolání poplachu. Zpravidla se umisťují pod povrch země, jsou tedy pouze pohledem nezjistitelné, nenarušují estetiku prostředí, uložení lze provést do jakéhokoliv materiálu, hlíny, štěrku, písku, betonu i asfaltu. Tím jsou zabezpečené i vůči sabotáži, detekční charakteristika je všesměrná, nelze se k nim tedy bez vyvolání poplachu ani podhrabat. Systém se skládá ze dvou částí, kabel vysílací a kabel přijímací, zpravidla jde o koaxiální kabely, jejichž stínění je sníženo štěrbinami v krytí, ty se postupně zvětšují se vzdáleností pro kompenzaci ztrát, umístěny jsou podélně vedle sebe v konstantní vzdálenosti. Umístěny by měly být na volném prostranství bez kovových a pohybujících se objektů, lze nastavit jejich citlivost odolnou vůči malým objektům/zvířatům, četnost planých poplachů je velmi nízká. Používají se ve dvou provedeních:

Provedení v dvojitém štěrbinovém kabelu

Je méně prostorově náročné, lze použít v omezeném prostoru. Vysílací i přijímací kabely jsou uloženy v jednom pouzdře, detekční zóna je zpravidla vysoká cca 1m a široká 2m, záleží i na hloubce uložení.

Provedení s dvěma štěrbinovými kabely

Kabely jsou umístěny zvlášť zpravidla ve vzdálenosti 2m od sebe v hloubce 25cm, detekční zóna je cca 1m vysoká a až 3m široká. Jeden úsek může být o délce 100 až 200m a lze tak střežit i několik km.

Obr. 7 Systém štěrbinových kabelů [29]

2.4 Mikrofonní kabely

Nachází uplatnění v aplikacích s nejvyšším stupněm bezpečnostních rizik, slouží jako ochrana perimetru objektu. Zpravidla se instaluje na pletivové, svařované a prefabrikované betonové oplocení. Je schopno zachytit jakýkoliv náznak útoku/sabotáže, řezání, střihání, roztahování apod. Ke snímání akustický projevů a převodu zachvění citlivého mikrofonického kabelu na elektrický signál se využívá mikrofonních kabelů s diskrétními snímacími prvky a mikrofonních koaxiálních kabelů s rozloženými snímacími parametry.

Mikrofonní kabely s diskrétními snímacími prvky

Záchvěvy detekují zpravidla pomocí elektretového mikrofonu v liniovém (úsekovém) provedení instalovaném na pletivovém oplocení. Zachytávaný signál je následně vyhodnocován ve vyhodnocovací jednotce, kterou doplňuje meteorologická jednotka snímající povětrnostní podmínky, které jsou tak kompenzovány za účelem omezení planých poplachů.

Mikrofonické koaxiální kabely s rozloženými snímacími parametry

Stav pletiva je sledován namáháním koaxiálního kabelu, na jehož výstupu vzniká elektrický signál, který je vyhodnocován s průběhem charakterizujícím způsob namáhání. Tento signál je zpracováván procesorovou jednotkou tzv. adaptivními algoritmy uloženými v paměti, díky čemu je spolu se senzorem aktuálních povětrnostních podmínek omezena možnost planých poplachů. Instalace tohoto systému je nenáročná pouze za pomocí plastových příchytek každých cca 30cm na stabilní oplocení. Jedna vyhodnocovací jednotka dokáže sledovat až 300m úsek, v případě dvou zónové až 600m.

Obr. 8 Instalace mikrofonního kabelu [24]

2.5 Otřesové detektory

Slouží zpravidla pro střežení plášťů budov, hlídají průrazy stěn, střech a stavebních konstrukcí sledováním a vyhodnocováním otřesů v konstrukcích ve sledovaném prostředí. Dělí se na dva typy: vibrační, seismické. Liší se především v citlivosti a způsobu vyhodnocování a tím i aplikací. **Seismické detektory** jsou podstatně citlivější, zachytí sebemenší záchvěvy v materiálu. Obsahuje také pokročilejší vyhodnocovací jednotku, která omezuje vznik planých poplachů, reaguje tak až při opravdových překonáváních mechanických zábranných systémů. Uplatnění mají zejména při střežení trezorů, trezorových skříní apod. **Otřesové detektory** jsou oproti seismickým o několik řádů méně citlivé, reagují na podstatně vyšší amplitudu vibrací a nedisponují tak pokročilým vyhodnocováním, reagují při určité úrovni vibrací. Zpravidla chrání materiály jako sklo, plech, dřevo, beton aj., které dobře přenášejí vibrace, vzduch ne. Střežit obvykle dokáží prostor v oblasti do několika metrů dle tvrdosti materiálů, měkčí do cca 3m a tvrdší až cca 6m.

Hlavním prvkem otřesových detektorů je senzor, který zprostředkovává přenos vibrací dál k vyhodnocení, zároveň určuje vlastnosti detektoru. Pracují na základě různých mechanických či fyzikálně chemických principech. Převážně se jedná elektrické principy, které umožňují miniaturizaci příslušných obvodů a zároveň dosahují vysokých citlivostí a přesností.

Mechanický měnič

Otřesové detektory obsahující mechanický měnič fungují na principu setrvačnosti pružně uchyceného závaží, kdy při dostatečném vychýlení způsobenému rozvibrováním chráněného povrchu dojde k rozpojení zabezpečovací smyčky a tím k aktivaci poplachu. Lze nastavit citlivost na sílu vibrací pomocí justačního (přidržovacího) šroubku. V klidovém stavu jde o uzavřenou smyčku, kterou prochází stálý proud do vyhodnocovací jednotky, jednotlivé detektory se připojují sériově. Jsou odolné vůči elektromagnetickému rušení z okolí, to je činí vysoce bezpečnými.

Elektroakustický měnič

Dnes se již tento typ běžně neinstaluje, lze se s ním setkat spíše u starších instalací PZS. Vibrace jsou opět snímány přímým kontaktem z chráněné plochy a to za pomocí akustického měniče, který má větší šířku frekvenčního pásma.

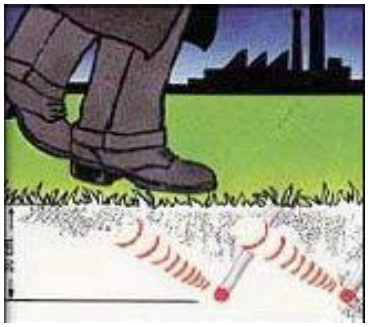
Piezoelektrický měnič

Tento typ otřesového detektoru využívá známého piezoelektrického jevu, při kterém je užívaný piezoelektrický materiál tedy krystal, který reaguje na vnější neelektrické podměty a to fyzickou deformaci, při níž je indukováno napětí, po navrácení do původního stavu napětí opět zaniká (funguje i obráceně). Dál jsou tyto elektrické signály zpracovávány a vyhodnocovány ve vyhodnocovací jednotce.

2.6 Zemní tlakové hadice

Jsou detektorem venkovní perimetrické ochrany známé též pod názvem GPS (Ground Perimeter System), jde o podzemní hydraulický systém realizovaný dvěma paralelně položenými pružnými hadicemi pod stálým tlakem ve vzdálenosti zhruba 1m od sebe v hloubce několika desítek cm napuštěnými nemrznoucí směsí. Principálně fungují tak, že detekují změny tlaku z prostředí, jež jsou způsobovány vnějšími podněty (chůze, přejezd auta,…). Změny tlaku jsou přenášeny do vyhodnocovacího senzoru, kde jsou následně převáděny na elektrické signály, pokud dojde k překročení určité prahové hodnoty, je vyvolán poplach.

Ukládají se zpravidla do vrstvy písku, což chrání vnější plášť hadic před ostrými předměty a kameny, jelikož jsou skryty pod zemí, jsou tak chráněny před zrakem útočníka, estetika povrchu není narušena, výhodou je možnost kopírování terénu jak výškově tak i půdorysně. Úseky jsou zhruba o délce 100 až 200m pokud je vyhodnocovací jednotka umístěna do středu. Lze systém „namnožit“ na více řad dvojic hydraulických tlakových hadic, čímž se rozšíří pokrytí, a také pak lze detekovat i směr pohybu narušitele. Instalace je složitější, je třeba dbát na okolní prostředí, rušit může okolní doprava atp., dále je třeba neumisťovat v těsné blízkosti stromů, jejich kořeny při kymácení způsobují tlak na okolí a vyvolávají falešné poplachy. Dále je třeba pravidelná kontrola stavu hadic, vnitřní tlak je zaznamenáván elektronikou.



Obr. 9 Ilustrace zemních tlakových hadic [34]

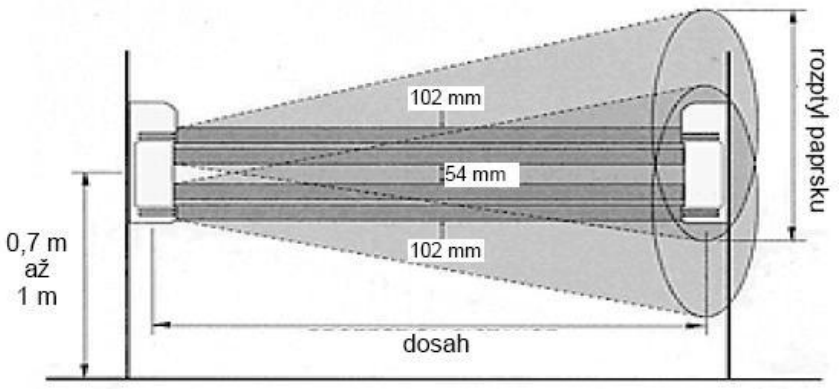
2.7 Vláknové optické systémy

Jedná se o moderní technologii umožněnou s příchodem optických kabelů, které jsou uloženy pod povrchem země, jedná se o vedení neelektrické, má tedy velmi vysokou odolnost vůči elektromagnetickému rušení a jsou pasivní, tedy nedetekovatelné. Zdrojem světla je IR dioda vysílající do vedení periodický signál z obou stran, v jádře o tloušťce od 100 μm vyrobeném ze skla dochází k interferencím, při jejich změnách dochází k vyvolání poplachu. Změny interferencí jsou vyvolány mechanickými změnami v prostředí, jde o velmi citlivou metodu, detekuje sebemenší pohyb, ohyb, vibrace, citlivost lze nastavit, ty jsou pak vyhodnocovány ve vyhodnocovací jednotce. Vyhodnocování je velice přesné, lze snadno určit, v jaké vzdálenosti došlo k narušení. V případě zvýšení počtu optických vláken lze určit i směr pohybu narušitele. Délka takového vedení může v současné době mít i desítky km.

Obr. 10 Instalace vláknového optického systému [26]

2.8 IR závory a bariéry

Jsou jedny z nejpoužívanějších venkovních perimetrických detektorů, skládají se z vysílací a přijímací strany. Mezi vysílačem a přijímačem probíhá jeden nebo více synchronizovaných či nesynchronizovaných IR paprsků, ty jsou vysílány pulzně pro zvýšení odolnosti vůči cizím světelným zdrojům. K vyhlášení poplachu dojde tehdy, je-li jeden nebo více paprsků přerušeno, záleží dle nastavení citlivosti, to neustále sleduje vyhodnocovací jednotka. Citlivost detekce lze nastavit dle doby přerušení paprsků např. ptactvem a jinými zvířaty. Dále moderní detektory obsahují obvody pro úpravu intenzity paprsků dle povětrnostních vlivů a vnitřní vyhřívání chránící před vlhkostí a námrazou, což zvyšuje příkon zařízení. Dosah paprsků udávaný výrobci je 60 až 250 i 300m pro klasické a 2 až 6m pro lištové, ty slouží k ochraně oken a dveří, instalují se zpravidla z vnější strany, ale lze je umístit i mezi okno a okenici. Montáž klasických detektorů je náročnější, terén musí být naprosto rovný bez překážek, jednotlivé úseky se musejí překrývat, aby nedošlo k tzv. mrtvým bodům. Nejnákladnější na instalaci jsou výkopové práce pro kabely, samotné detektory se umisťují na sloupky či zeď, zpravidla několik nad sebou, proto jsou vybaveny volbou z několika modulačních kmitočtů, aby nedocházelo ke vzájemnému ovlivňování.



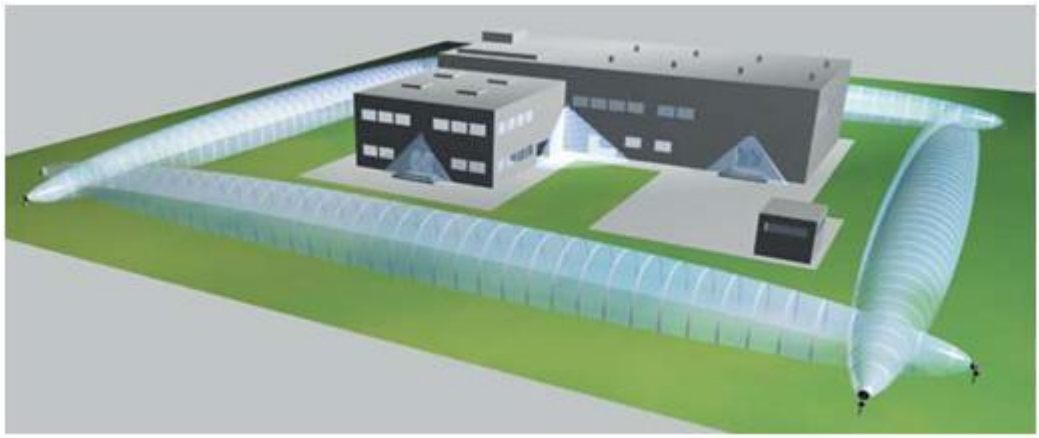
Obr. 11 Instalace IR závor a bariér [16]

2.9 Mikrovlnné bariéry a radary

2.9.1 Mikrovlnné bariéry

Mikrovlnné bariéry jsou prvky venkovní perimetrické ochrany, skládají se z vysílací a přijímací části, mezi přijímačem a vysílačem je vytvořeno elektromagnetické pole ve tvaru elipsy, při jehož přerušení či změně dojde k vyvolání poplachu, to snímá a

vyhodnocuje přijímací část. Patří tak mezi detektory aktivní vytvářející si své vlastní pracovní prostředí. Elektromagnetické pole bývá dnes standardně o frekvenci okolo 10GHz ± 0,5GHz, výjimečně 24GHz, zpravidla lze nastavit z několika frekvencí tak, aby se navzájem detektory nerušily. Vůči elektromagnetickému rušení z okolí je toto pole modulováno a dále jsou detektory vybaveny obvody kompenzujícími proměnlivost povětrnostních vlivů. Dosah bývá od několika desítek metrů zhruba do 300m. Narušení je detekováno změnou amplitudy, tato změna je odvislá od proporcionálního zastínění a tak je možno rozlišit různé typy objektů a narušení. K vyvolání poplachu dojde i při zvýšení intenzity signálu či rušení jiným zdrojem. Lze nastavit i citlivost a tak zamezit planým poplachům např. zvěří apod. Důležitá pro efektivnost systému je montáž, mezi vysílačem a přijímačem musí být přímá viditelnost, v okolí nesmí být pohybující se objekty (ploty, stromy, keře, tráva,…). Dále je třeba dodržovat zásady vyzařovacího diagramu a prvky umisťovat do takové výšky, aby nebylo možné chráněný úsek podplazit.



Obr. 12 Instalace MW bariér [35]

2.9.2 Mikrovlnné radary

Na rozdíl od bariéry nemají vysílač a přijímač zvlášť ale v jednom prvku, neustále vysílá do prostředí elektromagnetické záření o vysokých frekvencích (2,5GHz, 10GHz, 24GHz) a využívá Dopplerova jevu, tedy vyhodnocuje změny signálu odraženého ku vyslanému. Tyto změny jsou vyvolávány pohybem ve střeženém úseku, směrem k detektoru frekvence narůstá a naopak směrem od detektoru klesá, v těchto směrech je tedy tento typ nejcitlivější. Při použití více prvků je nutné je synchronizovat tak, aby nepracovaly na stejných nebo velmi blízkých frekvencích, které by je navzájem ovlivňovaly. Dosah a vyzařovací charakteristika se liší dle typu, dosah od jednotek metrů

po několik desítek metrů, vyzařovací charakteristika dle využití prstencová, doutníková či širokoúhlá.

2.10 Přístupové systémy

2.10.1 Základní pojmy biometrie a autentizace

Biometrie je věda zabývající se studií živých organismů, zejména člověka. Zkoumá měřitelné charakteristiky, jeho anatomické a fyziologické vlastnosti a v neposlední řadě také jeho chování, kde jde o tzv. behaviorismus. Což je přístup k psychologii zakládající na tvrzení, že lze chování zkoumat vědecky bez ohledu na vnitřní duševní stav subjektu, používá laboratorní metody výzkumu, je tedy považován za objektivní.

Hlavní význam této studie je rozpoznání osob dle jedinečných proporcí, křivek a charakteristických vlastností daného jedince za účelem identifikace porovnáním nasnímaných biometrických dat se všemi vzorky uloženými v databázi.

Takováto činnost je nazývána verifikací, při které dochází k potvrzení či vyvrácení identity zkoumané osoby. Což je činnost sahající daleko do historie, lidé vždy vše ve svém okolí včetně sebe navzájem identifikovali dle vizuálů, vzhledu tváře, charakteristický prvků v chování. Toto vše zdokonalil příchod moderních technologií resp. automatizace a rozvoj počítačových technologií dovolující daleko přesnější metody při rozpoznávání.

2.10.2 Autentizace

Je taktéž metoda identifikace osoby, jejíž součásti je zisk či odepření oprávnění k danému úkonu. Využívána je např. u automatizovaného docházkového systému, přístupového systému kontroly vstupů, výdejového či jiného informačního systému.

2.10.3 Metody autentizace

Heslem – Je to nejjednodušší a také nejvyužívanější metoda autentizace, využívá se všude v informačních počítačových systémech s nízkým stupněm zabezpečení. Jde o určitou posloupnost určitého počtu znaků, které zná nejlépe jen jedna konkrétní osoba. Nevýhodou je možnost dekódování speciálními programy, úroveň bezpečnosti tak záleží na délce a složitosti hesla jako jsou střídání velkých a malých písmen a užití číslic či jiných

speciálních znaků. Taktéž by nemělo být nikde poznamenáváno a nemělo by mít souvislost s osobou vlastníka ani jeho okolí a obměňováno by mělo být v určitých intervalech.

Předmětem – Přístup zajišťuje vlastnictví identifikačního předmětu tzv. tokenu nesoucí informaci nutnou pro autentizační protokol, která je co nejobtížněji kopírovatelná. Obvykle jde o magnetické či elektronické karty nebo čipy. Většinou je tato metoda kombinována se zadáním hesla popř. PINu.

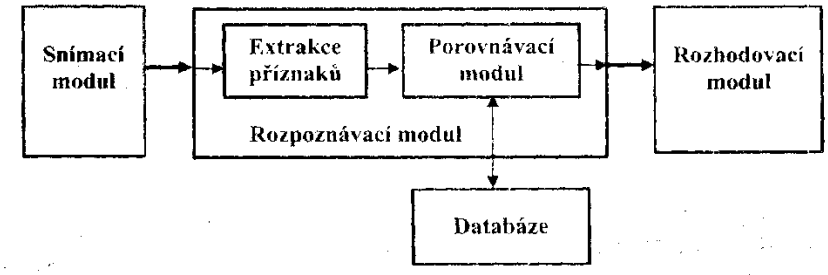
Biometrika – Využívá k autentizaci jedinečných tělesných prvků, odpadá tak nutnost zapamatování si hesla či neustálého nošení identifikačního předmětu. Také napodobení či zcizení je znesnadněno či vyloučeno. Konkrétní metody biometrické identifikace viz dále.

2.10.4 Biometrické systémy řízení a kontroly vstupů

Systémy řízení a kontroly vstupů v bezpečnostním průmyslu (ACS – Access Control Systems) kontrolují vstupy do chráněných objektů a prostor, vstup povoluje pouze osobám ověřeným při autentizaci. Proto obsahují biometrické přístupové systémy dva funkční režimy, prvním je registrační, při kterém jsou snímána biometrická data s účelem uložení do databáze a druhým je autentizační sloužící k identifikaci osoby na základě porovnání sejmutých biometrických dat s databází. K udělení oprávnění dojde po ověření naskenovaného vzoru se vzorem uloženým v databázi. Pro bezpečnost je důležité omezit počet nezdařených pokusů o přihlášení, než dojde k zablokování přístupu a popř. vyvolání poplachu jako pokus o neoprávněné vniknutí. Tento počet je důležité nastavit s ohledem na požadovanou úroveň bezpečnosti systému, čím nižší počet je zvolen, tím je větší pravděpodobnost falešných poplachů při nezdařené verifikaci. Je ale důležité nastavit takový počet pokusů, aby neoprávněný uživatel měl co nejmenší šanci získat dostatek informací o systému vedoucím k prolomení.

Přístupové systémy se také liší způsobem ukládání do databáze, buď přímo v zařízení anebo na vzdáleném serveru. U vysoce zabezpečených systémů by měly být ukládány i výsledky provedených verifikací. Zde se nabízejí tři možnosti a to přímo do zařízení, vzdáleného počítače či přímo do tokenu, pokud je použit. Ukládání přímo do jednotky snímače má nevýhodu omezené kapacity pro data, ale také z hlediska jednoduššího přístupu narušitele k uloženým datům. Při ukládání na vzdálený počítač odpadá omezení kapacitou, stále ale zůstává možnost průniku do systému zvenčí, je tedy nutno zabezpečit samotnou databázi. Posledním způsobem je ukládání záznamů přímo do tokenu, který též obsahuje jen omezenou kapacitu, ale také se zvyšuje jeho elektronická

složitost a tím i cena. Systémy ACS spadají pod normu ČSN EN 50133 (ČSN EN 50133-1 Systémové požadavky, ČSN EN 50133-2-1 Všeobecné požadavky na komponenty, ČSN EN 50133-7 Pokyny pro aplikace).



Obr. 13 Schéma biometrického ACS [7]

2.10.5 Bezpečnost biometrických systémů

Efektivnost biometrických rozpoznávacích systémů lze měřit z hlediska mnoha statistických koeficientů. Charakteristickými výkonnostními mírami jsou koeficienty nesprávného přijetí, nesprávného odmítnutí, vyrovnané chyby, doba zápisu etalonu a doba ověření.

Důvodem ke zvyšování bezpečnosti biometrických systémů je to, že přes jedinečnost biometrických příznaků pracují biometrické systémy s určitou chybovostí. Dalším důvodem jsou již zaznamenány případy napadení biometrických systém, objevují se pokusy o kopii otisků prstů, či plastické operace tváře. Jedním ze způsobů, jak bezpečnost zvýšit je aplikace ezoterické identifikace, jež se specializuje na znaky skrytého charakteru, např. žilního řečiště, pachu, DNA, ucha, podélného rýhování nehtu, termografických snímků, jež lze změnit obtížně nebo vůbec. Druhým způsobem je aplikace kombinovaných biometrických systémů, nejčastěji otisk prstu a geometrie obličeje, oční duhovky a charakteru hlasu. U kombinovaných biometrických systémů je pak výsledná pravděpodobnost přijetí neoprávněné osoby rovna součtu jednotlivých pravděpodobností biometrických metod.

False Acceptance Rate (FAR)

FAR koeficient udává pravděpodobnost toho, že neoprávněná osoba bude považována za osobu oprávněnou. Proto má FAR velký význam na míru bezpečnosti, může vést ke vzniku závažných škod.

$$FAR = \frac{N_{FA}}{N_{IIA}}.100[\%]$$

N_{FA} - počet chybných přijet

N_{IIA} - počet všech pokusů neoprávněných osob o identifikaci

False Rejection Rate (FRR)

FRR koeficient udává míru pravděpodobnosti pro chybné odmítnutí oprávněné osoby. Udává míru hlavně komfortu, neoprávněné odmítnutí je pro uživatele nepříjemné. Jde o chybné odmítnutí osoby, jež je v systému registrována jako oprávněná.

$$FRR = \frac{N_{FR}}{N_{EIA}}.100[\%]$$

N_{FR} – počet chybných odmítnutí

N_{EIA}- počet všech pokusů oprávněných osob o identifikaci

Failure to Enroll Rate (FTE nebo FER)

Udává poměr osob, u kterých došlo k selhání procesu sejmutí příznaku. Má vztah jak k osobě, tak snímané biometrické vlastnosti. K získání statistického údaje je zapotřebí velkého množství pokusů. Čím větší počet, tím přesnější výsledek.

$$FER(n) = \frac{pocet\_úspěspěšných\_pokusů\_o\_zápis\_u\_jedné\_osoby}{celkový\_pocet\_zápisů\_u\_jedné\_osoby}$$

False Identification Rate (FIR)

FIR koeficient udává pravděpodobnost, že při procesu identifikace je snímaná biometrická veličina nesprávně přiřazena k některému referenčnímu vzorku.

False Match rate (FMR)

FMR koeficient udává poměr neoprávněných osob, které jsou během srovnávacího procesu nesprávně identifikovány jako akreditované. V porovnání s koeficientem FAR se liší v tom, že na rozdíl od FAR se do FMR nezapočítávají odmítnuté pokusy z důvodu špatné kvality sejmutého obrazu.

False Non-Match Rate (FNMR)

FNMR koeficient udává poměr toho, že oprávněné osoby byly nesprávně rozpoznány během srovnávacího procesu. V porovnání s FRR se liší tím, že se nezapočítávají odmítnutí z důvodu špatné kvality sejmutého obrazu.

2.10.6 Metody biometrické identifikace

2.10.6.1 Geometrie obličeje

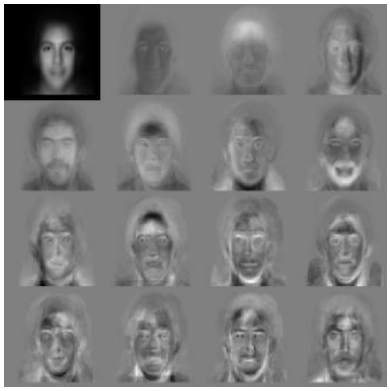
Problematika verifikace dle obličeje je jedna z nejvíce zkoumaných metod současnosti, proto se neustále vyvíjí a zdokonaluje. Rozpoznávání je založeno na srovnávání získaného snímku tváře s obrazem uloženým v databázi, tento způsob identifikace osoby porovnává tvar obličeje a významné body tváře, jako jsou oči, nos, ústa.

Základní rozdělení této metody je na statickou a dynamickou. U statické identifikace si je tohoto aktu osoba vědoma, snímání je prováděno z čelního úhlu za určitého nasvícení a rozlišení pořizovaného snímku. Účelem dynamické metody je schopnost snímat a rozpoznávat osoby v davu lidí, toho je využíváno při zjišťování pohybu zájmových osob, jako jsou zločinci, teroristé nebo také pohřešované osoby. Tyto systémy jsou využívány na frekventovaných místech, např. letiště, nádraží, banky, obchodní centra, náměstí apod.

Tři hlavní nejvíce studované a prozkoumané algoritmy rozpoznání obličeje jsou: Analýza hlavních částí (PCA – Principal Components Analysis), Lineární diskriminační analýza (LDA – Linear Discriminant Analysis), Elastický srovnávací diagram (EBGM – Elastic bunch graph matching).

Analýza hlavních částí (PCA)

Metoda PCA využívá k tvorbě vzoru vhodného k srovnávání vektorů tváře odvozených z kovarianční matice pravděpodobnostní distribuční funkce. Každou tvář lze rozdělit na tzv. eigenfaces (vzor tváře – matice jasových úrovní) a ty lze pak zpětně složit. Každá jasová úroveň tváře je reprezentována pouze číslem nikoliv přímo obrazem. Jedna osoba může mít v databázi více vzorových snímků za různých stavů v době pořizování.



Obr. 14 Eigenfaces [13]

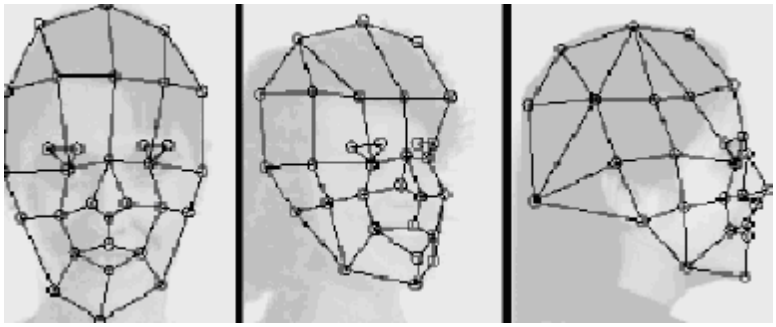
Lineární diskriminační analýza (LDA)

V metodě LDA jsou pořizované snímky tváří rozdělovány do skupin, kdy cílem je maximalizace rozdílů mezi jednotlivými skupinami a zároveň minimalizování rozdílů v dané skupině.

Obr. 15 Příklad roztřízení dle LDA [13]

Elastický srovnávací diagram (EBGM)

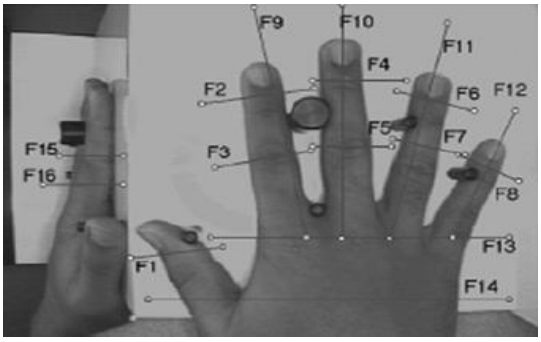
Metoda EBGM byla vyvinuta, jelikož předešlé metody nejsou schopné uvažovat nelineární charakteristiky, jako je osvětlení, pozice hlavy či výraz tváře. Na tváři jsou nadefinovány uzlové body, které jsou následně propojeny a tím definují linii tváře v prostoru, tím vznikne souřadnicová síť tváře. Rozpoznávání je poté realizováno pomocí filtrů uzlových bodů snímané tváře, které systém porovnává s databází a vyhodnocuje, celý proces trvá v řádu jednotek sekund. Problémem je přesnost určení orientačních bodů na tváři, proto je kombinována s metodou PCA nebo LDA. FRR: <1%; FAR: 0,1%



Obr. 16 EBGM souřadnicová síť tváře [13]

2.10.6.2 Geometrie ruky

Není příliš jedinečnou biometrickou charakteristikou, její využití v bezpečnostním sektoru je omezeno požadovaným stupněm bezpečnosti. Využívána zejména tam, kde je vyžadována rychlost verifikace, jde o kontaktní metodu. Zařízení využívá jednoduchého principu trojrozměrného snímání délky, šířky, tloušťky a povrchu ruky konkrétní osoby umístěné na vysoce odrazivém podkladu s pěti polohovými kolíky pro prsty s využitím kamery s CCD čipem a soustavy zrcadel. Zkoumaný snímek je černobílý, nehty se neměří. Metoda je také odolná na zašpinění rukou, charakteristika ruky je během života stálá, avšak může dojít ke změně tloušťky či jiným změnám, jako jsou zranění. Nevýhodou je i velikost snímací plochy oproti identifikaci otiskem prstu. FRR: <0.1%; FAR: 0.1%



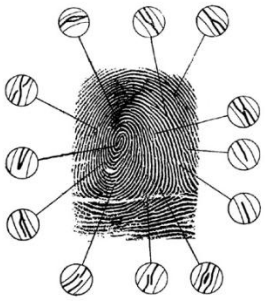
Obr. 17 Geometrie ruky [13]

2.10.6.3 Otisk prstu

Jedná se o daktyloskopickou metodu, zkoumá papilární linie na vnitřních stranách článků prstů, dlaní a chodidel. Jde o jednu z nejstarších, nejznámějších a nejrozšířenějších metod hlavně díky své spolehlivosti a rychlosti a jednoduchosti sejmutí vzorků. Neexistují na světě dva lidé, kteří by měli stejné tvary papilárních linií, navíc jsou po celý život relativně neměnné a lze je jen složitě odstranit, muselo by dojít k až k zasažení zárodeční

tkáně. Ke změnám může dojít při zraněních či opotřebení jako důsledku z vykonávané práce.

Tato metoda je využívána ve velkém množství odvětví, jako jsou různé bezpečnostní a informační systémy, ale i v kriminalistice, kde se velmi osvědčila a obsahuje již rozsáhlé databáze.



Obr. 18 Papilární linie [36]

Klasické snímání daktyloskopických stop

Pomocí inkoustu a papíru – Používá se pouze ve forenzní sféře policií při vyšetřováních, k sejmutí stačí pouze papír a inkoust, prstem namočeným do inkoustu se po papíře roluje tak, aby byl otisk získán celý s co největším počtem markant, aby byla jeho identifikace co nejrychlejší. Do elektronické podoby jsou jednoduše opticky naskenovány obrazovými snímači.

Bezprostřední (interaktivní) snímání daktyloskopických stop

Tento způsob je využíván zejména v komerčním bezpečnostním sektoru a to v přístupových systémech do objektů, metoda je vhodná i co se týče velikosti snímací plochy. Zkoumaná osoba přikládá prst na snímací plochu, která je mezičlánkem pro převod dat do elektronické podoby.

Rozdělení dle kontaktu při snímání:

Senzory kontaktní – Při snímání otisku prstu je nutný kontakt se snímací plochou.

- Optické – Snímaná plocha je zespod osvětlována laserovým paprskem a jsou zachycovány odrazy pomocí CCD prvku.

- Elektronické – Snímají elektrické pole vytvořené mezi dvěma vodivými deskami, prstem a senzorem. Nereaguje na špínu a drobné poškození povrchu kůže, proniká hlouběji pod povrch.
- Opto-elektronické – Kombinace optické a elektronické, snímací plocha vyrobena z TFT, který po doteku generuje světlo. Zespod snímací fotodiody převádějící světelný signál na elektrický.
- Kapacitní – Snímáno měřením kapacity, povrch senzoru obsahuje vysoký počet vodivých ploch, při dotyku dojde k přemostění, poté se měří jednotlivé úbytky napětí, takto vznikne digitalizovaný obraz v 256 odstínech šedi. Nevýhodou je ovlivnění nečistotami a nízkou vlhkostí.
- Tlakové – Povrch senzoru je elastický piezoelektrický materiál, tlak vyvolá elektrický signál, z nějž je získán daktyloskopický otisk.
- Teplotní – Obsahuje velmi malé citlivé pyrodetektory snímající teplotní rozdíly sekvenčně, je zapotřebí přejet prstem po snímací ploše, ze které se obraz otisku poskládán postupně, je třeba se tento pohyb naučit. Díky zkoumání teploty tato metoda zaručuje kontrolu, zda otisk patří živé osobě.

Senzory bezkontaktní – Při snímání otisku není třeba kontaktu se snímací plochou.

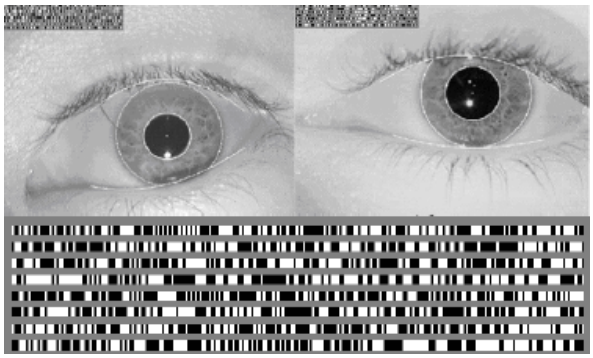
- Optické – Pracují na obdobném principu jako kontaktní jen s rozdílem schopnosti sejmout otisk na vzdálenost 3 až 5cm, odpadá tak znečištění snímací plochy nečistotami uživatelů.
- Ultrazvukové – Snímač vysílá generované zvukové vlny o vysokých frekvencích v řádech jednotek až několika desítek MHz a zaznamenávají odražené a deformované vlny na snímači umístěným kolmě k vysílanému paprsku na rotující hlavě. Výsledný obraz je trojrozměrný.

2.10.6.4 Duhovka oka

Jde o relativně nově vyvinutou technologii patentovanou teprve roku 1994. Duhovka má v oku funkci clony regulující velikost čočky na základě intenzity

dopadajícího světla na oko. Je považována za jednu z nejpřesnějších metod, duhovka je u každého člověka jedinečná, dokonce i u jednoho člověka je každá jiná. Vyvíjí se během prenatálního věku a její vzorkování je zcela náhodné, na zabarvení má vliv množství melaninového pigmentu.

Ke snímání oka je třeba kvalitní CCD kamera a neviditelný infračervený přísvit oka, pořizovány jsou snímky v odstínech šedi ve velkém rozlišení, které jsou digitalizovány do podoby fázových diagramů, ty pak slouží k vytvoření duhovkové mapy.



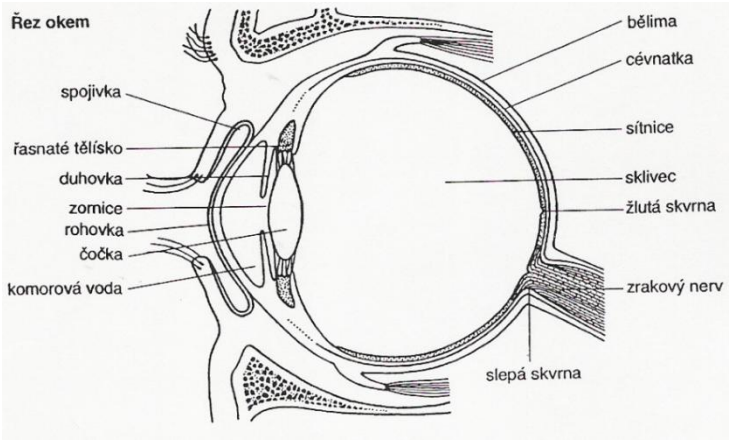
Obr. 19 Piktogram oční duhovky [13]

Předností této metody je bezesporu bezkontaktní sejmutí až na vzdálenost jednoho metru, překážkou nejsou ani brýle či kontaktní čočky, nelze přelstít fotografií. Jedná se tak o velice rychlou přesnou a pohodlnou metodu. FRR: 0,00066%; FAR: 0,00078%

2.10.6.5 Sítnice oka

Velice přesná metoda využívaná zejména v oblasti nejvyššího stupně zabezpečení, je zkoumána struktura cév v zadní části oční bulvy. K sejmutí je využíván opto-elektronický systém s infračervenou diodou vyzařující infračervený paprsek skrz zornici. Cévy sítnice paprsek odráží a vytváří tak rozpoznávaný snímek, samotná sítnice je průhledná.

Výhodou je vysoká přesnost, nevýhodou ale nízká uživatelská příjemnost, je nutno oko přiblížit k snímači na dobu až 15 sekund a sledovat jeden určitý bod, což může být pro osoby s různými očními vadami obtížné až zcela nemožné. Nelze aplikovat s nasazenými brýlemi. FRR: 0,4%; FAR: 0,001%



Obr. 20 Řez okem [37]

2.10.6.6 Akustická charakteristika hlasu

Metoda dříve využívaná převážně v kriminalistice, až nyní se dostává do soukromého bezpečnostního sektoru. Systém srovnává pořízený záznam s hlasovým vzorem uloženým v databázi. Jsou dva způsoby, osoba říká danou frázi nebo libovolnou frázi. Nelze překonat sebelepším imitátorem hlasu bez znalosti klíčové fráze. Při ověřování dochází k analýze amplitudově frekvenčního spektra měnícího se v čase, to je u každého člověka jedinečné. Hlas se během života u jednoho člověka mění, nejstálejší je v období mezi 20-60 let, vliv na to mají i nemoci. Charakteristické je svým zabarvením hlasu, intonací, rytmem, gramatikou, skladbou vět, na tom se podílí hlasový a vokálový trakt, ty se skládají z čelistí, rtů, zubů, jazyka, hlasivek, měkkého patra, dutiny ústní, nosní a dýchací svalstvo.

Nevýhodou je rozpoznávání hlasu v reálném prostředí, které je mnohem náročnější a v současné době neexistuje dostatečně přesný systém. Využití v soukromém sektoru má hlavně v telefonním bankovnictví a další vzdálený přístup k informačním systémům.

3 MATERIÁL NA TRHU

Sortiment bezpečnostních zařízení na trhu jsem čerpal především od dodavatelů bezpečnostních technologií v České republice, z nichž někteří mají pobočky též i v jiných zemích Evropy.

3.1 Distributoři v ČR a EU

ADI Global Distribution

ADI Global Distribution je součástí skupiny ADI, jednou z vedoucích firem v oboru distribuce zabezpečovacích a slaboproudých zařízení, která provozuje 32 poboček v 11 zemích v Evropě, na Středním východě a v Africe. [14]

Nabízí sortiment PZS, EPS, CCTV, EKV, domovních telefonů a videotelefonů, perimetrických systémů, datových komunikačních prostředků, včetně komplexních integrovaných řešení.

V České republice působí od roku 1991 pod značkou OLYMPO, jež byla roku 2003 převzata společností Honeywell divize Honeywell Security, která je součástí skupiny Automation and Control Solutions (ACS). Od ledna 2008 vystupuje pod značkou ADI Global Distribution. Kromě distribuce bezpečnostních zařízení též poskytuje návrhy řešení, školení, konzultace a technickou podporu včetně servisu.

Příkladné portfolio poskytovaných značek: Ademco, Honeywell, Optex, System Sensor, Indala, HID, Fermax a mnoho dalších.

EUROALARM, spol. s r. o.

Byla založena v lednu 1993 a patří bezesporu mezi přední dodavatele zabezpečovací techniky v České republice. Společnost je členem Asociace technických bezpečnostních služeb Grémium Alarm (AGA), Cechu EPS ČR, Profesní komory požární ochrany (PKPO), Hospodářské komory ČR a nadnárodní panevropské asociace Euralarm.

Společnost spolupracuje s obchodními partnery po celém světě a jako specializovaný velkoobchod zastupuje přední světové firmy vyrábějící systémy elektrické zabezpečovací

signalizace, kamerové a monitorovací systémy, systémy elektrické požární signalizace, stabilní hasicí zařízení, přístupové a docházkové systémy, evakuační systémy a veřejné ozvučení, nouzové osvětlení a vnější perimetrickou ochranu objektů.

Nabídku doplňuje široká škála instalačního materiálu, montážního příslušenství a speciální techniky. Je autorizovaným distributorem a značkovým servisem zabezpečovací a protipožární techniky, vyráběné předními světovými výrobci. [15]

EUROSAT

Eurosat CS spol. s r.o. je ryze česká obchodní společnost s více jak 15-ti letou tradicí, působící v oblasti zabezpečovacích a informačních technologií. [16]

Poskytují dodávku, montáž i servis poplachových zabezpečovacích systémů – PZS, Elektronických požárních systémů – EPS, Uzavřených televizních okruhů – CCTV, Systémů řízení budov, Přístupových systémů, Systémů evidence docházky, Systémů sledování mobilních objektů, Elektronických knih jízd Auto - GPS. Vedle toho poskytují i odborné certifikované školení.

STASANET

Opět poskytuje dodávku, montáž a servis (skrze montážní firmy) široké škály bezpečnostní technologií a vedle toho i školení. Též vydávají vlastní ucelený tištěný katalog s ceníkem zařízení. Jsou zaměřeni především na je monitorovací techniku (CNB, AV-Tech, Sentry 24…) videotelefony a domácí telefony (Commax, ACI Farfisa), elektronické zabezpečovací systémy (Paradox, Jablotron), IP kamery (Vivotek, ACTi) pohony pro brány a vrata (Proteco), docházkové systémy a specializovaný elektroinstalační materiál.

SEGURO

Společnost SEGURO se zabývá dovozem, distribucí a montáží i servisem satelitní techniky, autoalarmů, domácích audio a videotelefonů, zabezpečovacích, kamerových, přístupových a požárních systémů, měničů napětí, meteostanic, akumulátorů, baterií a nabíječů baterií, svítilen atd.

MARCOMPLET

Firma Pavel Procházka - MARCOMPLET je specializovaným velkoobchodním prodejcem komponentů měřící, regulační, topenářské a tlakové techniky. Základ prodeje tvoří výrobky od zavedených firem z oboru automatizační techniky, měření, regulace a vytápění jako jsou Belimo, ESBE, Sensit, Wilo, LDM, Grundfos,KSB, Regin, Fluke-Raytek, ZPA Ekoreg, Siemens, Olymp, ABB, Sauter, Metra Šumperk, Comet system, Emers, TG, Tork, Johnson controls, Mave, Oventrop, Honeywell, Heimeier, Huba cont., Rawet, AMIT, Giacomini, Buracco, Jablotron, TA Hydronics, Alco contr., Sigma Lutín, Danfoss, Ekorex, AM Technik, Augusta, SPA, SČA, Komextherm, Meibes. [19]

3.2 Výrobci zabezpečovacích zařízení

Vivotek Inc.

Společnost Vivotek byla založena roku 2000 sídlem na Taiwanu, od počátku se specializovala na integraci audiovizuálních a bezpečnostních zařízení do síťové infrastruktury. Postupem času se stále více orientuje na produkty pro zabezpečení, vlastní SoC (System on a Chip – integrovaný obvod) čipy jim umožňují implementaci pokročilých funkcí pro sledování, lepší využití přenosového pásma a zaručují nejvyšší možnou kvalit přenosu videa i audia v reálném čase. Z podporovaných funkcí lze zmínit formát streamingu RTSP s kodekem 3GPP/ISMA pro sledování obrazu i zvuku na mobilních zařízeních a streaming v několika různých kompresích současně.

Produkty poskytované společností Vivotek jsou IP kamery pro instalaci vnitřní i vnější a to v provedeních antivandal, minidome řady **MD**, dome řada **FD**, speeddome řady **SD**, PT řady **PT**, PTZ řady **PZ** s funkcemi den/noc, přísvitem (zpravidla IR LED, ale i bílou LED), několikamegapixelové, se zvukem, bezdrátovou komunikací přes WiFi a napájením PoE. Ke kompresi videa lze vybírat z kodeků MPEG, MPEG-4 a H.264 a snímacích čipů CCD, CMOS a WDR, což je variace na CMOS vyznačující se extrémním dynamickým světelným rozsahem. Dále společnost Vivotek poskytuje IP videoservery, IP Codery (záznamové zařízení NVR z vlastní produkce) a další výbavu jako IR přísvity, objektivy, stojánky, držáky, kabely PoE a vlastní softwarové řešení pro záznam a přehrávání.

AXIS Communications

AXIS Communications sídlící ve Švédském městě Lund bylo založeno roku 1984, v 90. letech se začali věnovat síťovým prvkům protokolu TCP/IP a v roce 1996 vydali na trh svoji první IP kameru NetEye 200. Od roku 2008 spolupracují se společnostmi Bosh a Sony na standardizaci rozhraní síťových produktů. V současnosti je společnost přítomna ve více než 30ti zemích světa s počtem zaměstnancům blížícím se jednomu tisíci, své produkty distribuuje zhruba do 70ti zemí, přes prodejce pak do více než 180ti zemi po celém světě. Jejich produkty jsou řešením pro profesionální instalace, jejich nabídku tvoří IP kamery v provedeních pro vnitřní i vnější instalaci a to jak fixní řady **M10, M11, P13, Q17**, tak pohyblivé PTZ řady **PTZ** i Dome řady **M30, M31-R, M32, P33** a kombinaci PTZ dome řady **P55, Q60**. Vybaveny mohou být i termovizí pro noční snímání (řada Q19) a rozlišovacími schopnostmi v řádech MPx. Dále jejich nabídka obsahuje video převodníky, audio video příslušenství a vlastní software pro správu videa.

Arecont Vision

Společnost Arecont Vision pochází z města Glendale na jihu Kalifornie, založena byla roku 2003 a již v roce 2004 přichází s první generací svých produktů, které se staly světově nejrychlejšími 2MPx IP kamerami na trhu celosvětově. Za 6 let své existence prochází společnost bouřlivým vývojem a přichází na trh s řadou výrobků, jež se stávají špičkou ve své kategorii IP kamer, ke snímání využívají čipy CMOS, soustředí se především na rozlišovací schopnosti, jež jsou v řádech MPx. Ke kompresi ve svých produktech využívají kodeků H.264 a MJPEG a to v řadách **MegaDome** s možností změny ohniskové vzdálenosti, PTZ, režimy den/noc, posílání několika streamů a v provedení antivandal pro vnitřní i venkovní instalaci. Řada **MegaVideo** je oproti předchozí uvedené řadě fixní, též umožňuje několik streamů při maximálním počtu snímků 32 za sekundu. Nejnovější řada, s logicky nejmenším počtem modelů, se nazývá **MegaView**, ta je určená pro nasazení v těch nejnáročnějších vnitřních i venkovních instalacích, obsahuje IR přísvit s udávaným dosahem až 25 metrů a 45°. Poslední řadou od Arecont Vision je panoramatické **SurroundVideo**, jež se sestavuje z čtyř 2MPx IP kamer v jednom krytu, jsou ve dvou provedeních a to v pokrytí okolí 180° a 360°, obrazový výstup jsou schopny poskytnout v počtu 22 snímků za sekundu.

Obr. 21 IP kamera Arecont Vision řady SurroundVideo [22]

Honeywell Security

Společnost Honeywell Security je mezinárodní konglomerátní společnost se sídlem v Morristown ve státě New Jersey v USA, založena byla již v roce 1906 a v současnosti zaměstnává přes sto tisíc zaměstnanců. Odvětví, na které se zaměřuje, jsou: letectví, automatizace a řízení, speciální materiály, dopravní systémy a výzkum a vývoj. Co se bezpečnostních systémů týká, dodává na trh své vlastní zabezpečovací ústředny, kamery včetně omezeného sortimentu IP kamer ve fixním, dome a PTZ provedení, záznamové zařízení DVR a různé detektory narušení. Z detektorů narušení lze jmenovat PIR **Activ8** pro vnitřní použití včetně funkce antimasking, dále duální PIR + MW detektory **DUAL TEC** opět včetně funkce antimasking. Dále vyrábí detektory tříštění skla FlexGuard, jež jsou základním prvkem plášťové ochrany, převážně v bezkontaktním provedení. V pasivním kontaktním provedení je pouze jeden s dosahem až 2,4m a to v kombinaci s magnetickým kontaktem. Ostatní detektory tříštění skla jsou pasivní bezkontaktní s dosahem 7,6 až 9m, jeden model je v provedení montáže na strop a jeden zápustný duální, jež nenarušuje estetiku prostředí. Dalším typem detektorů jsou otřesové detektory řady **SC** s poloměrem dosahu 1 až 5 metrů a čtyřmi nastavitelnými citlivostmi, vhodné jsou pro použitá na trezory, trezorové místnosti, zdi, bankomaty a depozitní sejfy. Model **SC105** navržený pro použití v hlučnějších prostředích jako obchodní centra, nádraží atd.

Dalšími výrobci otřesových detektorů na trhu je **Cosmotron řady VV** s dosahem až 14 metrů a nastavitelnými úrovněmi citlivosti. A s omezeným sortimentem **Optex Vibro, Texecom AEB, Risco RK, Paradox Safe Protector**.

Detektory tříštění skla pak dále vyrábí **Jablotron** a to model **GBS210** s detekční vzdáleností až 9m, **SENTROL INC.** s modelem **S5812** o dosahu až 7,5m a verzí s magneticky stíněným relé pro vyhodnocování tříštění skla napříč celým zvukovým spektrem. Dále **Texecom Limited IMPAQ GLASS BREAK** o dosahu až 9m a **PARADOX SECURITY SYSTEMS GLASSTREK 457** s nastavitelnou citlivostí 4,5 až 9m, detekuje dvě frekvence, při porušení skla a vlnu nárazu.

Otřesovými detektory se dále zabývá Cosmotron AB pod značkou UTC Fire & Security.

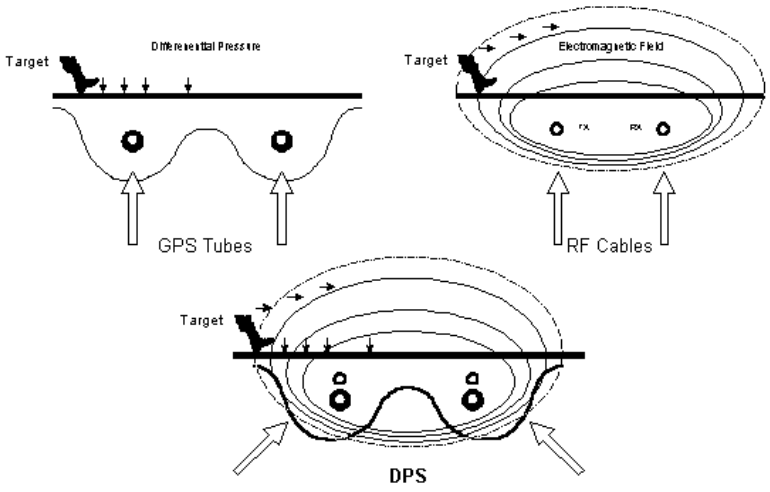
SENSTAR Corporation

Zabývá se již téměř 30 let výzkumem, vývojem a výrobou perimetrických detektorů narušení, dodávající do více než 80 zemí světa sídlem v Kanadě. Celkově jejich systémy střeží prostor více než 30 tisíc kilometrů zahrnující dopravu, vládní objekty, energetické zdroje, kritickou infrastrukturu, komerční objekty, VIP, vládní a právní budovy a nápravná zařízení a instituce. Štěrbinové kabely představuje řada **OmniTrax** jež je již 5. řadou, výška detekčního pole je zhruba 1m, šířka pak 3m o délce až 400m (při spojení dvou 800m). Obsahuje SW pro kalibraci citlivosti, stačí projít polem, dále SW dokáže zónu rozdělit až na 50 zón s přesností na 1m, 50 zón na jeden procesor. Tento systém je poskytován ve třech variantách, OC2 v provedení dvou štěrbinových kabelů o délkách 300 a 400m, SC1 v dvojitém štěrbinovém kabelu o délkách 50 a 200m a SC2 o dvou štěrbinových kabelech délek 50 a 200m. FAR méně než jednou za měsíc na jednu zónu. Je nástupcem předchozích produktů **Perimitrax** s délkou detekce 200m (400m při dvou zínách) a **Panther II** s délkou detekce 400m o dvou zónách. Mikrofonní detektory jsou pak reprezentovány řadami **FlexPS**, jež je nejnovější generací mikrofonního kabelu instalovaného na ploty o délce až 300m, jež je přímým nástupem řady **Intelli-FLEX**, má nízký počet falešných poplachů. Dalším zástupcem mikrofonních kabelů je řada **FlexPI,** jež je přizpůsobená pro vnitřní použití, určená k ochraně zdí, stropů, podlah a potrubí o délce až 600m. Dalším perimetrickým detektorem narušení určeným na ploty je řada **IntelliFIBER**, která se skládá z optického vlákna, jež reaguje na sebemenší ohyb.

Mikrovlnné bariéry společnosti Senstar jsou reprezentovány řadou **MPS** modely MPS-14000 o dosahu 457m, MPS-16000 o dosahu 5 až 183m, MPS-24000 o dosahu 3 až 150m a řadou **µltraWave**, jež je nejnovější generací o délce detekce 5 až 200m s digitálním zpracováním až 10 nastavitelných pracovních frekvencí. Posledním mikrovlnným detektorem značky Senstar je řada **The Revolution Radar** mající v současnosti 3 modely a to **R-7** o dosahu až téměř 700m (1,54km^2)**, R-14** o dosahu 1400m (6 km^2) a **R-28** o dosahu 2800m (24 km^2), avšak člověka detekuje pouze do 1900m, skenují plně 360° okolí každou sekundu.

Perimeterlarm

Perimeterlarm (GPS Perimeter Solutions/Systems) je malá dynamická švédská společnost zabývající se zemními perimetrickými systémy po dobu již 25 let celosvětově s velkými zkušenostmi s aplikací a instalací. Spolupracují dále s výrobci GPS Standard S.p.a. a Cias Elettronica Srl. Poskytují vláknové optické systémy **FPS** ve variantách **SNAKE**, které se instalují na ploty s dosahem 2km jedním průchodem a 1km dvěma průchody, dále **MILES** chránící potrubí o délkách až 25km a **SUN** určené k ochraně solárních elektráren před sejmutím solárních panelů s dosahem až 800m o maximálním počtu spojů 6. Dále se v jejich nabídce nacházejí perimetrické systémy plotové a to **CPS Plus**, jde o mikrofonní koaxiální kabel, dále **TPS** což je ostnatý drát detekující narušení střehem či jiným překonáváním, umisťují se 10 až 15cm nad sebe na sloupky vzdálené 2,5 až 3m od sebe. *Posledním plotovým detektorem je **WPS** používající ELCOS kabel s elektrickou charakteristikou reagující na deformaci.* Z perimetrických podzemních detektorů pak nabízí řadu **GPS Plus**, jde o zemní tlakové hadice vyhodnocující změny tlaku mezi sebou o délce maximálně 100m. Dále řada **PPS** je nástupcem předchozí uvedené, obsahuje pokročilé detekce, které jsou schopny určit narušení s tolerancí 5m na maximálně 200m dlouhém úseku za použití dvou tlakovacích soustav o počtu 20 zón. Řada **RFC** je příkladem štěrbinových kabelů o délce 100m na zónu. Poslední řadou je **DPS**, jež kombinuje řady GPS/PPS a RFC, tedy zemní tlakové hadice a štěrbinové kabely.



Obr. 22 Systém DPS od Perimeterlarm [25]

Optellios Inc.

Je společnost založená v roce 2000, od roku 2004 dodává na trh optické vláknové systémy pod názvem **FiberPatrol**. Model **FP1100-X** je určený pro ochranu plotů o maximální délce 16km, na každý kilometr lze nadefinovat až 31 zón o nepřesnosti 7 až 23m. Další model **FP1210/1220** je v samostatném provedení modulů v odolném panelu s procesorem schopným hlídat až 4 zóny, tento systém je vhodný pro instalaci na ploty i pod zem. Maximální délka zóny 8km, kabelu 48km. Model **FP2100-X** určený pro podzemní instalaci, má stejné vlastnosti jako model FP1100-X na ploty. Řada **FP3000** je určená pro ochranu zdí proti šplhání po zdi či průrazu zdi, maximální délka kabelu 96km, počet zón 31 na kilometr s přesnosti určení detekce 7 až 23m. Dále řada **FP6100-X** je určená pro ochranu potrubí o délce až 40km na prvek, maximální počet zón je 12 na jeden kilometr. Poslední řada od Optellios Inc. nese název **FP5000** a je určena k ochraně komunikačních sítí, tedy strukturované kabeláže o délce až 96km o maximálním počtu zón 31 na jeden kilometr. Model FP5100 je schopen vyhodnocovat a reportovat přesnou polohu narušení.

OPTEX Co., Ltd

Má 25 letou zkušenost v produkci pasivních i aktivních IR detektorech, které uvádí na trh do více než 50 zemí světa. Z aktivních IR závor jsou to řady **PHOTOBEAMS** s modely AX a BX s dvěma paprsky o dosahu 20 až 200m, volbou ze 4 kanálů, nastavitelností citlivosti na přerušení paprsků, montují se na zeď či trubku, jsou určeny pro třídu prostředí

IV. A řada **REDNET** s modely RN ve sloupkovém provedení výšky 1,75m s až 16 paprsky tvořící „síť“ s nízkou možností falešných poplachů o dosahu 25 až 150m.

Takenaka Engineering Co., Ltd.

Evropská pobočka TAKEX Europe Ltd. má 25 let zkušeností v oboru, na trh dodává detektor tříštění skla řady **Ultrasonic GS** s dosahem 7m vertikálně, 8m horizontálně, mikrovlnné detektory, PIR, požární hlásiče a především IR závory **Photoelectric Beams PB** s dosahy 20 až 200m v provedení s 2 nebo 4 paprsky u některých modelů včetně možnosti nastavení synchronizace.

Bunker Seguridad Electrónica S.L.

Je španělská společnost sídlem v Madridu, specializuje se na výrobu sloupků pro aktivní perimetrické IR bariéry Optex a Takex, které nabízí ve dvou provedeních, čistě průmyslové sloupky s IR řady **PT** (oboustranný), **MB** (jednostranný) výšek 0,5 až 3m. A zahradní sloupky pro obytné domy s osvětlením řad **MALTA**, **CAV**, **CAV-W** výšek 0,5 až 3m.

Southwest Microwave, Inc.

Americká společnost založená roku 1971, své produkty dodává do více než 80 zemí, soustředí se na mikrovlnné detektory, roku 1981 zakládá The Microwave Products Division (MPD). Na trh dodává i mikrofonní kabely pro ochranu plotů řad **INTREPID MicroPoint** 100 až 200m a **MICRONET**, dále dodává i štěrbinové kabely řady **INTREPID MicroTrack.** Mikrovlnné bariéry nesou označení **INTREPID MicroWave** pracující na frekvenci 24GHz s dosahem až 450m dle typu, umožňují výběr z 6 modulačních kanálů.

CoNet s. r. o.

Na českém trhu se objevili už v roce 1990 se zaměřením na elektroniku a výpočetní techniku, od kompletace počítačů postupně přešla na specializované činnosti v oblasti datových uložišť, profesionálních tiskáren, docházkových systémů, systémů čarového kódu

a distribuci dalších výrobků. Z přístupových systémů na základě biometrických metod na trh uvádí produkty **CoNetLock 240** a **260**. Model 240 je biometrická závora na otisk prstu, pracuje nezávisle na PC nebo síťových zařízeních, napájena je ze čtyř AA baterií. S kovovým tělem je vhodný pro vstupy do malých kanceláří, apartmánů nebo obytných domů. Dokáže zapamatovat až 30 otisků prstu. Zaregistrované otisky si pamatuje i po vyjmutí baterií, optický senzor rozpozná otisk prstu za dobu kratší než je jedna vteřina. Obsahuje též možnost odemčení pomocí klasického mechanického klíče. Model 260 je biometrický zámek, který nabízí 3 metody identifikace. První je otisk prstu, který je snímán rychlým optickým snímačem, zařízení může uložit do paměti až 50 uživatelů. Další metodou identifikace je pomocí PINu (až 30 PIN kódů), poslední způsob přístupů je klasický mechanický klíč.

e-Data

Objevili se na trhu před více než 20 lety, první přístupový systém uvedli před více než 15 lety, sídlí v USA v Texase a v Německu poblíž Stuttgartu. Na trh dodávají čtečku otisku prstu s dotykovou klávesnicí do venkovního prostředí **TLR401** podporující až 6000 uložených vzorků otisků prstů. Podporuje přenos vzorků otisku prstu navzájem mezi čtečkami, takže není zapotřebí registrovat uživatele v každé čtečce, dále podporuje ověření čipovou kartou i PIN kódem. Veškerá odezva okolo 1s.

Hyundai Hightech Inc.

Je jihokorejská společnost sídlící v hlavním městě Soul založena v roce 1990, Hyundai znamená korejsky moderní. Na trh dodává IT, bezpečnostní a měřící technologie. Z biometrických přístupových systémů na trh dodává **Biocav HDBFD-1000**, který zabezpečuje vchody nejen kódovým zámkem, ale také čtečkou otisku prstů. Celé vnější zařízení ochraňuje kvalitní kovový odlévaný kryt, který chrání i klávesnici se 12 tlačítky vybavenou podsvícením. Rozpoznání otisku prstu je prováděno optickou metodou, trvá méně než 1s, kapacita je 1000 otisků prstů. Uživatelské heslo ani otisk prstu nejsou smazány ani v případě vybité baterie.

4 CERTIFIKACE A ZKUŠEBNICTVÍ

Certifikát je obecně dokument prokazující nějakou skutečnost, vystaven musí být akreditovaným ústavem. Certifikované výrobky v ČR musejí splňovat podmínky českých technických norem (ČSN), které nejsou obecně závazné. Českých technických norem se především týkají **zákon č. 22/1997 Sb**. o technických požadavcích na výrobky a o změně a doplnění některých zákonů a zákon a **zákon č. 102/2001 Sb.** o obecné bezpečnosti výrobků.

Česká technická norma je dokument schválený pověřenou právnickou osobou (§ 5) pro opakované nebo stálé použití vytvořený podle tohoto zákona a označený písmenným označením ČSN, jehož vydání bylo oznámeno ve Věstníku Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví (dále jen "Věstník Úřadu"). Česká technická norma není obecně závazná. [12]

Nařízení vlády č. 17/2003 Sb. kterým se stanoví technické požadavky na elektrická zařízení nízkého napětí, obsahuje podmínky uvedení elektrického zařízení na trh, postup posuzování shody, označení CE a jiné označení. Obsahem podmínek uvedení el. Zařízení na trh jsou:

- Všeobecné požadavky
- Ochrana před nebezpečím, které může způsobit elektrické zařízení
- Ochrana před nebezpečími, která mohou vznikat působením vnějších vlivů na elektrické zařízení

Nařízení vlády č. 616/2006 Sb. o technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility udává požadavky na elektromagnetickou kompatibilitu (EMC).

Zařízení musí být navrženo a vyrobeno tak, aby bylo s přihlédnutím k dosaženému stavu techniky zajištěno, že

a) elektromagnetické rušení, které způsobuje, nepřesáhne úroveň, za níž rádiové a telekomunikační zařízení nebo jiné zařízení není schopné fungovat tak, jak má,

b) úroveň jeho odolnosti vůči elektromagnetickému rušení předpokládanému při používání k danému účelu mu dovoluje fungovat bez nepřijatelného zhoršení určených funkcí. [41]

Nařízení vlády č. 426/2000 Sb. kterým se stanoví technické požadavky na rádiová a na telekomunikační koncová zařízení.

CEN/CENELEC

European Committee for Standardization (CEN) je Evropská komise pro normalizaci založená v roce 1961, European Committee for Electrotechnical Standardization (CENELEC) Evropská komise pro normalizaci v elektrotechnice založená v roce 1959. Jsou to nezávislé neziskové technické organizace zřízené dle Belgického práva v Bruselu sdružující národní organizace pro normalizaci. CEN tvoří národní normalizační orgány na území všech zemí v EU a EFTA, CENELEC národní elektrotechnické normalizační orgány. Roku 1982 ve smlouvě o spolupráci se CEN/CENELEC prohlásili za „Společnou evropskou normalizační instituci“, ústřední sekretariáty obou jsou v Bruselu. V rámci zemí v EU tvoří požadavky na produkty, jako jsou společné úpravy požadavků na bezpečnost a zdravotní nezávadnost výrobků, minimální standardy ochrany spotřebitelů atd. Důvodem evropských norem je rychlejší sladění předpisů o produktech oproti národním normám.

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ), je organizační složkou státu v resortu Ministerstva průmyslu a obchodu ČR, jehož hlavním posláním je zabezpečovat úkoly vyplývající ze zákonů České republiky upravujících technickou normalizaci, metrologii a státní zkušebnictví a úkoly v oblasti technických předpisů a norem uplatňovaných v rámci členství ČR v Evropské unii, sídlí v Praze na Praze 2. Založen byl 1. ledna 2009 a nahradil dřívější Český normalizační institut (ČNI).

Ochrana utajovaných informací je zajišťována dle zákona č. 412/2005 Sb. Ta se skládá z personální bezpečnosti, průmyslové bezpečnosti, administrativní bezpečnosti, fyzické bezpečnosti, bezpečnosti informačních nebo komunikačních systémů, kryptografickou ochranou. Certifikace technických prostředků provádí Národní bezpečnostní úřad (NBÚ).

4.1 Zákon č. 22/1997 Sb.

Tento zákon upravuje:

a) způsob stanovování technických požadavků na výrobky, které by mohly ohrozit zdraví nebo bezpečnost osob, majetek nebo přírodní prostředí (dále jen "oprávněný zájem"),

b) práva a povinnosti osob, které uvádějí na trh výrobky, které by mohly ohrozit oprávněný zájem,

c) práva a povinnosti právnických nebo fyzických osob pověřených k činnostem podle tohoto zákona, které souvisí s tvorbou a uplatňováním českých technických norem (dále jen "normy") nebo se státním zkušebnictvím. [12]

Státní zkušebnictví

Státní zkušebnictví je soubor činností uskutečňovaných Úřadem a právnickými nebo fyzickými osobami pověřenými podle tohoto zákona, jejichž cílem je zabezpečit u výrobků stanovených podle tohoto zákona posouzení shody s požadavky technických předpisů. [12]

Certifikace

Certifikace podle tohoto zákona je činnost nezávislé autorizované nebo akreditované osoby, která vydáním certifikátu osvědčí, že výrobek nebo činnosti s výrobou související jsou v souladu s technickými požadavky na výrobky. [12]

Autorizace

Autorizací se pro účely tohoto zákona rozumí pověření právnické osoby k činnostem při posuzování shody výrobků stanovených podle tohoto zákona (dále jen "autorizovaná osoba"). Autorizaci pro činnost podle tohoto zákona uděluje na žádost rozhodnutím Úřad po dohodě s ministerstvy a jinými ústředními správními úřady, jejichž pravomoci se týká posuzování stanovených výrobků prováděné autorizovanými osobami. Nedojde-li k takové dohodě, rozhodne o autorizaci Úřad, jehož rozhodnutí může na

základě podnětu dotčeného ministerstva nebo jiného ústředního správního úřadu zrušit vláda. Úřad v rozhodnutí o autorizaci stanoví podmínky pro dodržování jednotného postupu autorizovaných osob při jejich činnosti a vymezí jeho rozsah. [12]

Prohlášení o shodě

Stanovené výrobky mohou výrobci nebo dovozci uvést na trh jen po posouzení shody jejich vlastností s požadavky na bezpečnost výrobků stanovenými tímto zákonem a technickými předpisy (dále jen "posouzení shody") způsobem odpovídajícím stanoveným postupům posuzování shody. [12]

Akreditace

Akreditací se pro účely tohoto zákona rozumí postup, na jehož základě se vydává osvědčení o tom, že právnická nebo fyzická osoba, která o ni požádala, je způsobilá ve vymezeném rozsahu provádět zkoušky výrobků, kalibraci měřidel a certifikační nebo jinou obdobnou technickou činnost. [12]

4.2 Přehled českých norem v PKB

Tab. 2 Přehled českých norem v PKB [4]

POPLACHOVÉ SYSTÉMY		+
Všeobecně EN 50130+	Poplachové systémy proti vniknutí a přepadení (I&HAS) (PZTS) EN 50131+	Systémy uzavřených televizních okruhů (CCTV) EN 50132+
Systémy kontroly a řízení vstupu (ACS) EN 50133+	Systémy přivolání pomoci (SAS) EN 50134+	Systémy tísňové (HUAS) EN 50135+ (sloučeno s 50131)

Přenosová zařízení (ATS) EN 50136+	Systémy kombinované nebo integrované (IAS) EN 50398+	Elektrická požární signalizace (EPS) EN 54+

Tab. 3 Skupina českých norem ČSN pro I&HAS [4]

Číslo normy	Zjednodušený název
EN 50131-1 ed. 2	Systémové požadavky
prEN 50131-2-1	Společné požadavky na detektory (příprava)
EN 50131-2-2	Pasivní infračervené detektory
EN 50131-2-3	Požadavky na mikrovlnné detektory
EN 50131-2-4	Požadavky na kombinované PIR a MW detektory
EN 50131-2-5	Požadavky na kombinované PIR a ultrazvukové detektory
EN 50131-2-6	Detektory otevření (magnetické kontakty)
CLC/TS 50131-3	Ústředny
EN 50131-4	Výstražná zařízení
CLC/prTS 50131-5-1	Společné požadavky pro propojovací zařízení (příprava)
EN 50131-5-3	Požadavky na zařízení využívající bezdrátové propojení
EN 50131-5-4	Propojovací zařízení využívající vf techniku
EN 50131-5-5	Propojovací zařízení využívající IČ techniku
EN 50131-6 ed. 2	Napájecí zdroje
CLC/TS 50131-7	Pokyny pro aplikace
CLC/TS 50131-7-1	Detektory rozbíjení skla (akustické)
CLC/TS 50131-7-3	Detektory rozbíjení skla (aktivní)
EN 50131-8	Zamlžovací bezpečnostní zařízení/systémy

Tab. 4 Skupina norem pro CCTV [4]

Číslo normy	Zjednodušený název
EN 50132-1	Systémové požadavky
EN 50132-2-1	Černobílé kamery
EN 50132-2-2	Barevné kamery
EN 50132-2-3	Objektivy
EN 50132-2-4	Příslušenství
EN 50132-3	Místní a hlavní řídící jednotka
EN 50132-4-1	Černobílé monitory
EN 50132-4-2	Barevné monitory
EN 50132-4-3	Záznamová zařízení
EN 50132-4-4	Zařízení pro okamžitý výtisk obrazu
EN 50132-4-5	Videodetektor pohybu
EN 50132-5	Přenos videosignálu
EN 50132-6	(volná)
EN 50132-7	Pokyny pro aplikace

5 VÝVOJOVÉ TRENDY A PROGNÓZA VÝVOJE

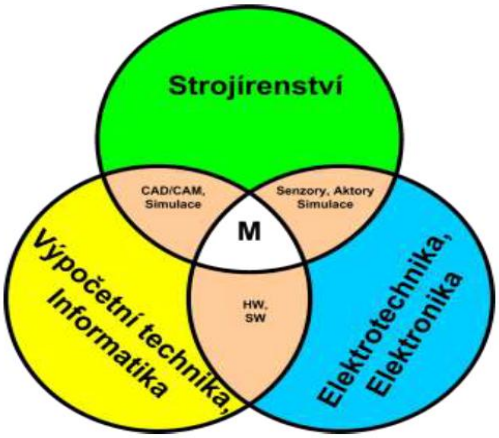
Současnými trendy výrobců zařízení bezpečnostních systémů je soustředění se především na spolehlivost a přesnost elektroniky, zejména pak eliminace planých a falešných poplachů např. vlivem prostředí a povětrnostními vlivy (meteorologické stanice, vyhřívání a další technické opatření). Dalším trendem je zdokonalování ochran před sabotážemi za pomoci mechaniky i elektroniky (např. odolnější kryty, laserové závor uvnitř venkovních sirén, při jejichž přerušení třeba pěnou dojde ke spuštění poplachu). V oblasti mechanických zábranných systémů jde o vývoj a zdokonalování stavebních materiálů z hlediska jejich fyzických vlastností.

5.1 Kamery CCTV

V případě kamer CCTV je směr vývoje jasný, jsou jím IP kamery díky svým pokročilým funkcím a neustále se vyvíjející video technologii (záznamu, zpracování i přenosu). Současné trendy jsou především navyšování rozlišovacích schopností kamery a tím schopnost zaznamenávat detaily dříve nemožné, dále rychlost pořizování snímků díky pokročilejší elektronice a snímacím čipům. Možnosti rozlišovacích schopností, počty snímků a kamer pak rozvíjí zdokonalující se přenosové cesty navyšující svou kapacity, zejména optické vlákna. Zároveň je věnována pozornost věcem jako stabilizace obrazu, schopnosti přibližování a PTZ. Ty jsou již často kombinovány s dalšími systémy jako PIR a další technologie, kdy se kamery natáčí za směrem narušení atp.

5.2 Mechatronika

Vývoj započal již během 70. let v Japonsku, přesto dodnes nemá stálou přesnou definici, jde však o spojení několika inženýrských oborů. Nejčastěji jsou zmiňovány obory strojírenství (mechanika), elektronika a výpočetní technika (softwarové inženýrství). Účel mechatronických zařízení je jejich automatizace sloužící k řízení systémů bez nutnosti zásahu člověka. Elektronická část tak slouží ke snímání stavu kontrolované veličiny, informatická část vyhodnocuje dané zjištění a mechanická část slouží ke korekci do požadovaného stavu. Využití tak nachází především u výrobních procesů díky své spolehlivosti, ekonomičnosti a programovatelnosti. Uplatnění ale již nachází i domácnostech za účelem řízení spotřebičů, zejména v instalacích tzv. inteligentních budov.

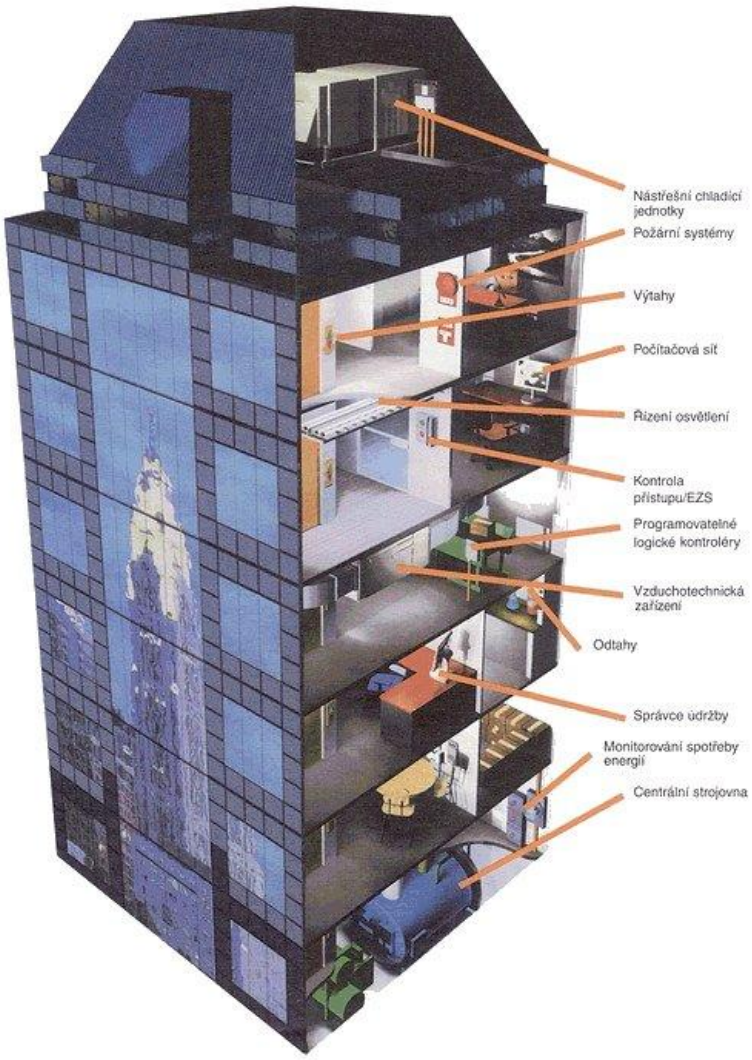


Obr. 23 Složky mechatroniky [38]

5.2.1 Inteligentní budovy

Inteligentní budovy jsou objekty s integrovaným managementem, tj. se sjednocenými systémy řízení (technika prostředí, komunikace, energetika), zabezpečení (kontrola přístupu, požární ochrana, bezpečnostní systém) a správy budovy (plánování, pronájem, leasing, inventář). Optimalizací těchto složek a vzájemných vazeb mezi nimi je zabezpečeno produktivní a nákladově efektivní prostředí. Inteligentní budova pomáhá vlastníkovi, správci i uživateli realizovat jejich vlastní cíle v oblasti nákladů, komfortu prostředí, bezpečnosti, dlouhodobé flexibility a prodejnosti. Inteligentní budova uspokojuje současné potřeby vlastníka a nájemce budovy a může být jednoduše přizpůsobena jejich rostoucím nárokům v budoucnosti, umožňuje úspory pořizovacích i provozních nákladů. [10]

Základními požadavky na inteligentní budovy jsou minimalizace energetických nároků a provozních nákladů, toho je docíleno integrací několika systémů (vytápění, vzduchotechnika, řízení osvětlení, výtahů, požární signalizace, zabezpečovací systém, přístupový systém, CCTV,…) do jednoho systému ovládaného automaticky z jednoho místa, dnes zpravidla modulárním či kompaktním programovatelným automatem, se kterým jsou spojeny všechny prvky pomocí datových sběrnic. Dříve byl tento systém výsadou velkých budov, dnes existují i systémy vhodné pro středně velké objekty, bytové domy, komfortní rodinné domy. Jejich součást je třeba zahrnout již do projektování, cenově jde o miliony pro větší objekty a statisíce pro menší.



Obr. 24 Příklad inteligentní budovy [10]

5.3 Biometrické přístupové systémy

V budoucnu určitě bude pokračovat rozšiřování přístupových systémů na základě biometrických metod díky svým přednostem oproti klasickým metodám (heslo lze rozluštit, čipové karty zkopírovat či ztratit). Odolnější jsou i z hlediska napadnutelnosti, které je složité i technicky náročnější. Za tímto účelem jsou již vyvíjeny biometrické autentizace podle tvaru žilního řečiště, rýhování nehtů, tvaru ucha, odrazu zvuku v ušním kanálku, tvaru a pohybu rtů, spektroskopie kůže, pachu, DNA a další, nazývané ezoterická identifikace. Tyto znaky je jen velice obtížné či zcela nemožné napodobit.

II. PRAKTICKÁ ČÁST

6 NÁVRH BEZPEČNOSTNÍHO ŘEŠENÍ

Tento návrh bezpečnostního řešení je pojat jako možné zabezpečení pláště budovy rodinného domu, tedy malého objektu s přilehlou oplocenou zahrádkou, situovaného do běžného městského prostředí za použití plášťové a perimetrické elektronické ochrany.

6.1 Popis objektu

Řešený objekt je fiktivní, avšak stavební projekt je na základě rodinného domu ROMAN od Luboše Purmenského. U mého fiktivního domu jde o moderní novostavbu rodinného domu s garáží v ceně několika miliónů Kč nově vybaveného nejmodernější spotřební elektronikou, obsahující rodinné šperky a cenné předměty historického typu (sbírka) a také firemní dokumenty uložené v trezoru. Dům je obýván středně velkou rodinou průměrného věku dospělých 40 let bez zdravotních komplikací. Stavba je umístěna ve středně velkém městě v obytné části dalších rodinných domů v blízkém okolí.

Obr. 25 Vzorový dům ROMAN [39]

6.2 Požadavky na návrh

Majitel požaduje zabezpečení domu i jeho přilehlého pozemku před pohybem nežádoucích osob, jelikož jde o nový dům moderně a draze vybavený, je požadována co nejrychlejší reakce systému na případné narušení bezpečnosti za účelem bezpečí pláště budovy. Dále nepožaduje žádné speciální úpravy a nastavení citlivostí na domácí zvířata, nemají a neplánují pořizování žádného většího zvířete. Jsou dány požadavky na dálkové ovládání brány vjezdu a garážových vrat.

6.3 Řešení návrhu

Stanovení stupně zabezpečení

Dle platné normy ČSN EN 50 131-1 ed. 2 stanovuji stupeň zabezpečení 2, tedy pro nízké až střední riziko a to z toho důvodu, že je sice předpokládaný pokus o útok na objekt za účelem zcizení výbavy či dokumentů, ale riziko není až tak vysoké, aby byl tento útok páchaný skrze střechu, postačí tedy efektivně navržený druhý stupeň. Sabotážní detektory jsou tak povinné pro tísňové prostředky a detektory vniknutí, nikoliv pro rozvodné krabice. Musí být detekováno otevření normálním způsobem a odejmutí z montážní plochy, změna orientace detektoru volitelná.

Střeží se	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Obvodové dveře	O	O	OP	OP
Okna		O	OP	OP
Ostatní otvory		O	OP	OP
Stěny			P	P
Stropy nebo střechy			P	P
Podlahy				P
Místnosti	T	T	T	T
Objekt (vysoké riziko)			*S*	*S*

O-otevření P-průnik T-past S - objekty vyžadující speciální pozornost

Obr. 26 Přehled zabezpečení dle stupně zabezpečení [2]

Stanovení třídy prostředí

Pro vnitřní prvky uvnitř objektu stanovuje dle platné normy ČSN EN 50 131-1 ed. 2 třídu prostředí I vnitřní vytápěné obytné s pracovními teplotami v rozsahu +5 až +40°C vyjímaje garáž, která nebude vytápěna, kde stanovím pro jistotu třídu II vnitřní všeobecné

s pracovní teplotou v rozsahu -10 až +40°C. Pro ostatní venkovní prvky stanovuji třídu IV venkovní všeobecné o pracovní teplotě -25 až +60°C.

Mimo elektronické zabezpečení objektu je počítáno také s mechanickým zabezpečením, jako je vyhraničení obvodu pozemku oplocením, v tomto případě plotem se zděným základem s kovovou výplní popř. dřevěnými plaňkami, kvalitními bezpečnostními dveřmi a kováním. V přední části domu, kde se nachází vstup a vjezd na pozemek z veřejné komunikace, bude obsahovat dálkově ovládanou bránu s elektrickým pohonem pro vjezd auta a branku se zvonkovým tlačítkem popř. domácím video telefonem a klasickým zámkovým systémem na mechanický klíč.

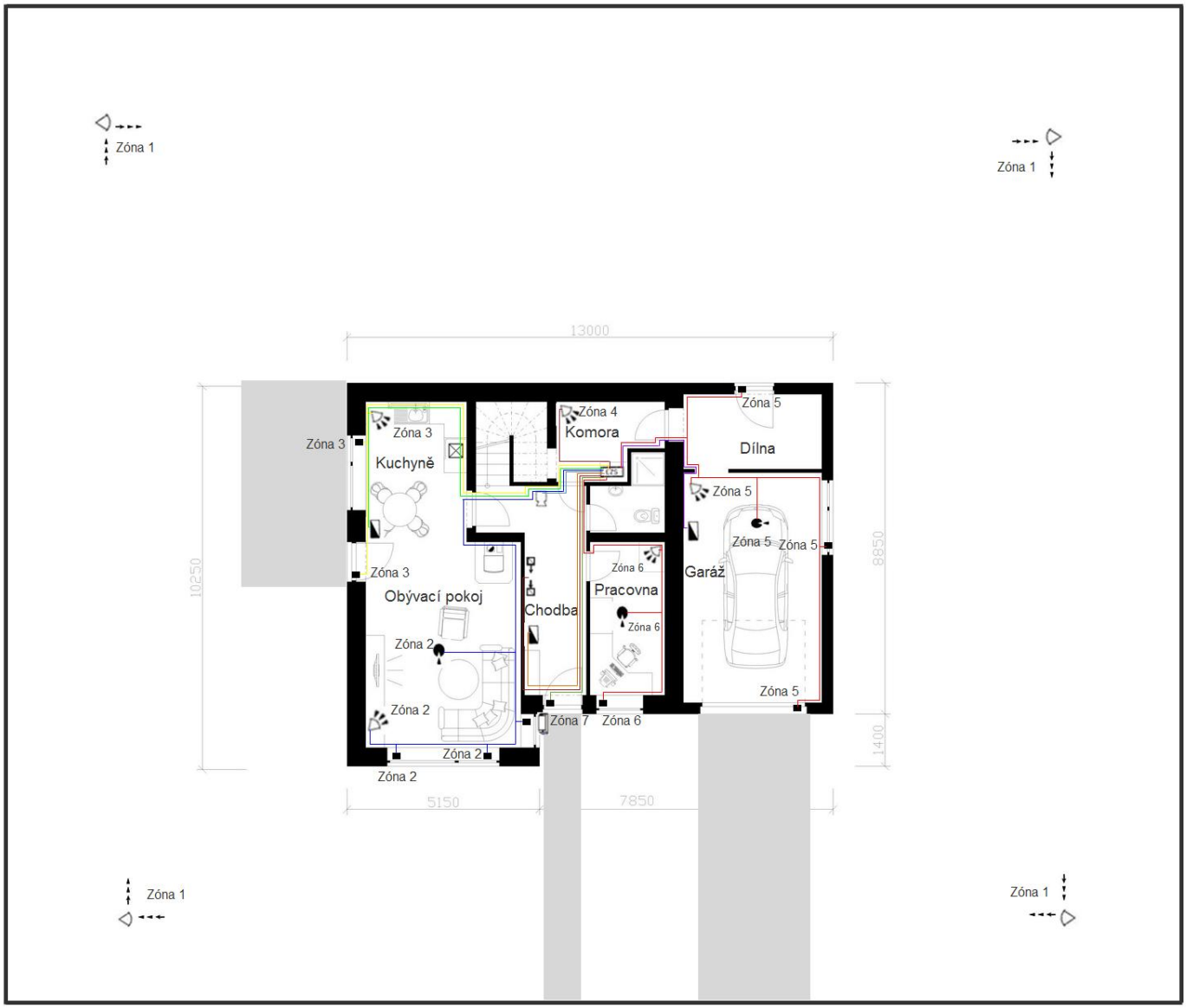
Vnitřní perimetr pozemku objektu budou chránit IR detektory instalované do krytu sloupků jako zahradní osvětlení, umístěny budou po obvodu plotu ve vzdálenosti zhruba dva metry. Každý sloupek s krytím do 180° bude obsahovat 4 až 6 IR závor tak, aby nebylo možné je podlézt ani přeskočit, sloupek obsahuje i tamper proti sabotáži otevřením krytu a je doplněn tamperem proti přelezení sloupku. Prostředí je nutno přizpůsobit tak, aby mezi IR závorami nezavazely žádné objekty.

Možnou variantou je i využití štěrbinových kabelů uložených v zemi, z důvodu omezeného prostoru lze využít variantu v dvojitém štěrbinovém kabelu, kde je vysílací i přijímací kabel v jednom pouzdře. Podmínkou je vyčištění terénu od pohyblivých a kovových objektů.

Další možnou vhodnou variantou místo IR závor jsou optické vláknové systémy nevyzařující elektromagnetickou energii do okolí umístěné v zemi, jsou skryté a prakticky nedetekovatelné, podmínkou je umístění dál od stromů, aby nebyly vyvolávány vlivem tlaků kořenů od povětrnostních podmínek plané poplachy.

Samotný plášť budovy budou chránit magnetické kontakty na bočních a zadních dveřích osazených klasickými zámky na mechanické klíče a na všech oknech proti jejich nežádaným otevření. Dále budou všechna okna a prosklené dveře pokryty bezkontaktními pasivními detektory tříštění skla proti narušení skleněné výplně. Hlavní dveře budou mechanicky odolné bezpečnostní ovládané přístupovým systémem na základě biometrie člověka konkrétně otisk prstu popř. v kombinaci s možností klasického mechanického

klíče či PIN kódu. Garážová vrata budou dálkově ovládaná klíčenkou stejně jako vjezdová brána, s elektrickým pohonem a chráněná magnetickým kontaktem.



Obr. 27 Návrh zabezpečení objektu v přízemí [39]

Obr. 28 Návrh zabezpečení objektu v 1. patře [39]

6.4 Soupis navrhnutých prvků

Ústředna PARADOX Digiplex EVO-48/4PGM

Z nabídky systémů DIGIPLEX EVO je tato ústředna svým rozsahem, nicméně poskytuje komplexní řešení zabezpečení pro střední i rozsáhlejší objekty včetně zabudovaného systému pro kontrolu přístupu.

Parametry a funkce

- 48 zón, 4 podsystémy
- vstupů s ATZ = až 16 zón na základní desce
- rozšiřování zón
- 96 uživatelských kódů
- až 127 modulů na sběrnici

- políčkové programování a upgrade firmware
- Software Winload / NEware
- 1024 událostí v paměti s datem a časem
- délka sběrnice: 900m
- napájení 16V~, spínaný zdroj 1,7A odběr ústředny cca 100mA
- 4 PGM výstupy (optorelé 50mA, spínají na +/-) + 1 relé 5A, 24V [17]

IP komunikátor PCS300

PCS300 je univerzální IP (Internet Protokol) přenosový modul, který umožňuje zabezpečovací ústředně přenos událostí na pult centralizované ochrany pomocí IP protokolu přes internet nebo pomocí GPRS. PCS300 se dodává ve dvou provedeních.

- PCS300 s GPRS12 - modul má GPRS / IP modul

- PCS300 bez GPRS12 - modul má jen IP modul

PCS300 se připojí k jakémukoli komunikátoru (RING, TIP) ústředny a zachycuje přenosové kódy v Contaktu ID. Podporuje dvě komunikační sekvence, každá z nich je vázána na konkrétní telefonní číslo. Veškeré programování PCS300 se provádí přes webové rozhraní, buď vzdáleně přes Ethernet IP, nebo přímým připojením k PC.

Parametry a funkce

- 128-bitové (RC4 a MD5) nebo 256-bitové (AES) šifrování
- Napájení 12V DC (z ústředny nebo samostatného zdroje)
- Odběr 150 mA, max. 300 mA při GPRS / GSM přenosu [16]

Modul rozšiřující počet drátových zón ZX8

Sběrnicový modul rozšíření systému pro 8 zón. Modul lze připojit kamkoliv na sběrnici a má plně programovatelné zóny.

Parametry a funkce

- Napájení 9V - 16V
- Proudový odběr max. 28mA
- Vyvážené vstupní zóny > 8
- PGM výstupy:1

- Počet zón: 8, 16 se zdvojením ATZ [16]

Bezdrátový obousměrně komunikující modul MG-RTX3

Bezdrátový obousměrně komunikující modul (na frekvenci 868MHz a 433MHz) kompatibilní se systémy ESPRIT (lze použít jenom klíčenky), SPECTRA SP a DIGIPLEX EVO (pro tyto systémy použitelný kompletní sortiment vysílačů). K modulu jsou připojitelné výhradně vysílače řady MAGELLAN. Modul může být použit i samostatně (tj. bez připojení k ústředně).

Parametry a funkce

- 32 bezdrátových zón
- napájení: 11-16V=, odběr: max. 140mA
- obousměrná komunikace po sběrnici na frekvenci 433MHz
- plovoucí kód, kryptovaný přenos
- detekce rušení signálu, a měření síly signálu
- až 4 PGM výstupy [17]

IR závora OPTEX AX-130TN

Řada AX-TN jsou dvoupaprskové infrazávory s mrazu odolným krytím IP65. Všechna citlivá místa, jako otvory pro šrouby, kudy by mohl vniknout prach, voda nebo hmyz, jsou utěsněny gumovými vložkami. Tím je zajištěna vysoká spolehlivost ve venkovním prostředí. Kromě toho je vzdálenost mezi horní a spodní optikou a šířka paprsků pečlivě navržena tak, aby poskytovala nejideálnější detekční pole a předcházelo se tak falešným poplachům detekováním pouze narušitelů.

Skládají se z optického vysílače a přijímače. Umožňují natočení úhlu. Přídavná TX jednotka pro ochranu tamperu, ochrana vůči přepětí. Snadné nastavení, instalace a elegantní design.

Parametry a funkce

- Dosah ve venkovním prostředí 40 m
- Krytí IP65
- Instalace na sloupek (ø 32 až 48 mm) nebo na rovný povrch

- Možnost vložení vyhřívací jednotky HU-3
- Automatická regulace citlivosti
- Pryžové těsnění zajistí úplnou prach těsnost a zabrání vniknutí vody
- Možnost nastavení doby přerušení paprsků 50 / 100 / 250 / 500 ms
- Přesné nasměrování úzkých, ostře ohraničených paprsků
- Ochranný kryt se stříškou zabraňuje vzniku námrazy na krytu spodního paprsku
- Horizontální a vertikální nasměrování paprsků
- Běžný provoz až do 99% úniku paprsků, tzn., že ani husté sněžení, déšť nebo mlha nesníží funkčnost detektoru
- Ochrana vůči přepětí až 14 kV
- Doba přerušení paprsků Volitelná mezi 50,100,250,500 ms
- Napájení 10,5 až 28 V DC
- Max. odběr 41 mA
- Doba sepnutí poplachu 2 sek. (±1)
- Poplachový výstup NC, max. 28 V ss / 0,2 A
- Tamper NC sepne při otevření krytu max. 28 V ss / 0,2 A
- Vlhkost prostředí Max. 95%
- Natočení paprsků ±90° horizontálně, ±5° vertikálně
- Umístění - Vnitřní / venkovní: na stěnu / na sloupek
- Pracovní teplota -30°C až +60°C [14]

Zahradní svítidlo s prostorem pro IR závory Bunker Seguridad MALTA

Samostatně stojící zahradní svítidlo výšky 1,85 m s prostorem pro montáž max. 6 vysílačů nebo přijímačů IR závor AX-TN/TF(BE) a PB-TK/TE. Montáž na betonovou patku (buď prostřednictvím konzoly MAFB nebo pomocí vhodných kotev).

Parametry a funkce

- Možný rozsah směrování IR závor 180 °
- Rozměry - výška 1850 mm [14]

Magnetický kontakt USP-500SP

Čtyř drátový polarizovaný hliníkový příložný magnetický kontakt s armovanou hadicí pro plošnou montáž především na vodivé materiály. Montážní podložka je součástí dodávky. Vodiče jsou pevně zality v kontaktu a jsou chráněny armovanou hadicí.

Parametry a funkce

- Pracovní mezera 20 mm
- Typ smyčky NC
- Tamper [16]

Vratový magnetický kontakt USP-3000

Kovový magnetický kontakt USP-3000 je masivní kontakt určený pro velké dveřní systémy a vrata. Kabel tohoto magnetu je ochráněn pancéřovým krkem, který je tak chráněn před porušením.

Parametry a funkce

- drátové vývody v pancéřovém krku
- možnost přejezdu automobilem bez poškození
- 2 - drátové provedení
- Pracovní vzdálenost 57 mm [16]

Samo závrtný magnetický kontakt USP-A1D

Výhodou tohoto samo závrtného magnetického kontaktu je především jeho velikost. Díky jeho klínovitému tvaru a samo závrtnému provedení jej jednoduše upevníte například do dřeva (velikost díry 3/8"; cca 9.5mm) nebo do tenčích kovových zárubní či okenních rámů.

Parametry a funkce

- životnost 100 miliónů sepnutí
- NC kontakt
- Pracovní vzdálenost 15 mm [16]

Detektor tříštění skla GlassTrek 457

GLASTREK 457. Jedná se o nový vylepšený vysoce kvalitní a 100% spolehlivý detektor, plně otestovaný přímo při výrobě. Dva provozní režimy (adresace pro DIGIPLEX EVO série nebo konvenční relé provozu). Detektory detekují dvě frekvence, vzniklé při porušení skla. Nízkofrekvenční vlnu nárazu a vysokou frekvenci tříštění skla. Nevzniknou-li tyto dvě frekvence současně, nedojde na detektoru k vyhodnocení poplachu. Glastrek se hodí k použití pro detekci rozbití klasických skleněných tabulí, temperovaného, nebo laminovaného skla. Při použití nejsou nutná žádná další nastavení. Glastrek musí být instalován na pevné ploše, bez otřesů a chvění.

Parametry a funkce

- frekvenčních digitálních filtrů, digitální zesilovač a odhad kolísání frekvence
- Audio výstup pro monitorování zvuku
- Nastavitelná citlivost pro vzdálenost od 4,5 do 9 m
- Napájení 9 -16 V DC
- Odběr 25 mA
- Operační teplota - 20 ˚C do + 50 ˚C [16]

PIR detektor DGP2-50

Pasivní infračervený pohybový detektor s duálním prvkem. Tento detektor je vybaven patentovanou technologií "Digital Motion Detection" zajišťující vysokou spolehlivost přímým A/D převodníkem a technologií automatického čítače pulsů.

Parametry a funkce

- Oboustranná komunikace s ústřednou Digiplex pomocí BUS sběrnice
- Přímý převod z analogového PIR senzoru na digitální signál a následné zpracování
- Jednoduché nebo duální vyhodnocování signálu
- Digitální automatický čítač pulsů 5 úrovní
- Vysoká odolnost proti elektromagnetickému rušení
- Digitální teplotní kompenzace
- Typ senzoru PIR duální
- Geometrie senzoru Obdélníkový
- Digitální protichůdná detekce NE

- Počet detekčních zón 25
- Pracovní teplota bez kondenzace - 20 až + 50 ˚C
- Výška instalace 2 - 2,7 m
- Napájení 9 - 16 V ss, max 15 mA
- Hlídaná plocha 9 x 9 m
- Vlhkost 95% [16]

Bezdrátový detektor kouře SD-738

Bezdrátový vysoce citlivý opticko - kouřový detektor sloužící jako doplněk zabezpečovacího systému PZS. Pracovní frekvence detektoru je 433 MHz nebo 868 MHz. Uvnitř vestavěna siréna pro akustické spuštění poplachu.

Kouřové detektory série SD jsou navrženy tak, aby splňovaly nejpřísnější normy požární bezpečnosti a spolehlivě detekovali vznikající požární nebezpečí. SD série využívá multisenzorové technologie spolu s pevně nastavenou teplotní hranicí detekce požáru. Proces výroby těchto kouřových detektorů podléhá systému ISO9001:2000.

Parametry a funkce

- Dosah v zástavbě 30 m s MG6060/6160 nebo 60 m s modulem MG-RTX3/RCV3
- Vlhkost Od 10 do 85 %
- Napájení 9 V baterie
- Životnost baterií 18 měsíců při normálních podmínkách s alkalickými bateriemi [16]

Dotyková LCD klávesnice TM4

TM4 je dotyková barevná grafická LCD sběrnicová klávesnice, barevný širokoúhlý displej s úhlopříčkou 10.9cm, programovatelné názvy pro zóny, podsystémy, uživatele a PGM výstupy, slot na externí paměťovou SD kartu pro nahrávání vlastních témat a zvuků, fotografií pro použití s funkcí slide show a pro modernizaci firmware. Vestavěný senzor pro měření, zobrazení vnitřní i venkovní teploty a vlhkosti, zákaznické překlady prováděné pomocí webové aplikace. V provedení bílé nebo černé.

Parametry a funkce

- Širokoúhlý 10,9cm jasně ostrý barevný displej
- Nastavitelné dotykové plochy pro zóny, podsystémy, uživatelů a programovatelných výstupů
- Slot paměťové SD karty pro nahrání vlastních témat obrazovky, zvuků, fotografií a pro servisní aktualizaci
- Vstup pro externí teplotní detektor pro měření venkovní teploty
- Ovládání programovatelných výstupů
- Napájení: 11 - 16 V=
- Proudový odběr: max. 110 mA
- Displej: barevný 16-bit, 54 x 95 mm
- Rozlišení displeje: 480 x 272 bodů
- Typ zóny na klávesnici: NC, bez hlídání tamperu
- Prohlížení historie událostí: ano
- Zvonkohra zóny: ano [16]

Grafická LCD klávesnice Grafica

Grafica je posledním krokem v posloupnosti vývoje klávesnic zabezpečovacích systémů. Grafica umožňuje nejen zobrazení vytvořených plánů budovy s detektory, ale zjednodušuje ovládání pomocí grafického menu a navigačních tlačítek. Vnitřní software obsahuje více než 120 000 řádků zdrojového kódu a je cíleně vytvořen pro maximální komfort cílového uživatele. Programovací software umožňuje plnou konfiguraci, včetně downloadu bitmap a melodií. Konstrukce využívá nejnovějších technologií konstrukce základní desky, moderní kovový design, texty kláves tvořené pomocí laseru.

Parametry a funkce

- Okamžité a přehledné zobrazení zóny na příslušném půdorysu při poplachu, přemostění nebo otevřených zónách při nastavování systému
- Zobrazení zóny blikáním při současném vypsání jména zóny a zobrazení aktuálního stavu
- Popis jednotlivých funkcí umožňuje jednoduchou zprávu uživatelů a nastavování parametrů systému

- 15 editovatelných melodií pro příchod, odchod, poplach a speciální událost
- Nastavení až 8 speciálních událostí s melodií a grafickým zobrazením na displeji
- Možnost upgrade software
- Podporuje maximálně 96 zón
- Nastavení zvonkohry nezávisle pro každou zónu s možností použití časovače
- Proudová spotřeba 130 mA
- Ochranný kontakt ANO
- Sběrnicový adresovatelný modul ANO, lze připojit kamkoliv do sběrnice systému Digiplex
- Programování pomocí klíče, klávesnice, software Winload, kopírováním z jiné klávesnice
- Provozní napětí 12 až 16 V ss
- Provozní teplota 0˚ až + 50˚ C [16]

Dotyková LCD klávesnice K656

Parametry a funkce

- Dotykové klávesy s podsvícením
- Zobrazení zón
- Použití v systému: ovládací, programovací
- Napájení: 11 - 16 V
- Proudový odběr: 80mA - 120 mA
- Displej: dvouřádkový, 32 znaků
- Prohlížení historie událostí: ano [16]

Vnější zálohovaná siréna PARADOX PS-128

PARADOX PS 128 je venkovní zálohovaná siréna, která patří mezi špičkové výrobky. Obsahuje výstup REPORT, který umožňuje předávat do ústředny informace o stavu baterie, reproduktoru a světla. Další inovací je servisní vstup sirény, který přepíná sirénu do servisního módu, ve kterém lze sirénu bezpečně otevřít a jakkoliv s ní manipulovat. Mód úspory energie zabraňuje úbytku na zvukové a světelné intenzitě a prodlužuje životnost baterie. Pokud je při první montáži nízké napětí na baterii, siréna vás na to

upozorní tichým dlouhým signálem a nezačne pracovat dokud baterie nebude poskytovat požadované napětí.

Pravidelným monitorováním stavu baterie systém dokáže předcházet jejímu úplnému vybití. Při detekci příliš nízkého napětí baterie totiž siréna přechází do úsporného režimu. Kromě testu baterie je vyhodnocován i stav reproduktoru a světla, přičemž test baterie je prováděn v intervalech 6h nebo 24h podle nastavení jumperu, zatímco světelný a reproduktorový test probíhá neustále. Stav výstupu Report je však aktualizován jen v okamžiku testu baterie.

Parametry a funkce

- Siréna je uložena v protipožárním krytu, který má vnitřní ocelovou krabici upravenou proti násilnému vniknutí a odtržení
- Vysoce efektivní reproduktor o výkonu 40 W
- Vydává hlasitý zvukový efekt 128 dB / 900 - 2400 Hz
- Napájení 13,6 - 14,8 V
- Baterie12 V / 1,2 až 7,0 Ah
- Minimální napětí baterie 9,8 V
- Typ světla 12 V / 18 W
- Odběr v klidu 5 mA
- Průměrný odběr reproduktoru 1,2 A
- Maximální odběr 2,8 A
- Typ ochranného kontaktu NC [16]

Vnitřní siréna SA-105

Velmi výkonná piezoelektrická siréna, kterou lze použít do vnitřního prostoru, kde vytváří nesnesitelnou hlukovou bariéru, i do motorového prostoru vozu.

Parametry a funkce

- Napájení 6 až 16 V
- Odběr 250 mA
- Akustický výkon 120 dB/m [42]

Biometrický elektronický zámek Biocav HDBFD-1000

BioCav je moderní biometrický elektronický zámek, který zabezpečuje vchody nejen kódovým zámkem, ale také čtečkou otisku prstů.

Vnější jednotka:

- Celé vnější zařízení ochraňuje kvalitní kovový odlévaný kryt, který chrání i klávesnici
- Klávesnice se 12 tlačítky je vybavena podsvícením - aktivováno po stisknutí prvního tlačítka.
- Senzor otisku prstu je zapuštěn do dutiny uvnitř krytu

Vnitřní jednotka:

- Dvě ovládací tlačítka: ZAMKNOUT / ODEMKNOUT
- Manuální páka pro odemčení / zamčení
- Tlačítka pro "naprogramování" přístroje (nastavení kódu, vložení otisku prstu)
- Duální zámek

Parametry a funkce

- Otevření pomocí otisku prstu
- Otevření heslem
- Jestliže je baterie vybitá, uživatel může otevřít dveře pomocí pohotovostního terminálu
- Pokud jsou dveře otevřeny abnormálním způsobem, systém aktivuje alarm
- Uživatelské heslo ani otisk prstu nejsou smazány ani v případě vybité baterie
- rozpoznání otisku prstu optická metoda
- rychlost ověření méně než 1 vteřina
- poměr chybných zamítnutí méně než 0,01%
- poměr chybných přijetí méně než 0,0001%
- registrační kapacita 1,000 otisků prstu
- baterie 1,5 V alkalická baterie 4 kusy (AA)
- životnost baterie více než 5,000 krát použitelné
- pracovní teplota -20°C – 65°C
- vlhkost 10% - 90% [28]

Dálkový ovladač MG-REM2

Parametry a funkce

- Podporuje Stay D (od verze 2.0 a výš)
- Ovládání až šesti funkcí
- Informace o stavu systému
- Zpětná zvuková vazba
- Dosah v typické zástavbě:
- 45 m s MG-RTX3
- RF frekvence 433 MHz nebo 868 MHz [16]

6.5 Výstup návrhu

Tato práce byla pojatá jako bezpečnostní návrh a nikoliv projekt, při převádění do praxe by jej tedy bylo třeba dále doplnit o nezbytné součásti projektů. Jako návrh by jej tedy šlo dále upravovat dle požadavků zadavatele práce a dále různě konfigurovat.

Na požadavky fiktivního zadavatele jsem tedy provedl bezpečnostní návrh pro fiktivní rodinný dům v městské části rodinných domů. Požadavkem bylo zabezpečit plášť budovy a její okolí (perimetr), pro ochranu perimetru jsem zvolil praktickou a nenáročnou možnost a to aktivní IR závory podél vnitřní strany oplocení, které by nemělo být narušováno zvenčí. Počet IR závor byl zvolen tři dvou paprskové nad sebou, aby nebylo možné jejich překonání ani podplazením, či přeskočením a instalovány byly do praktických zahradních osvětlení výšky 2m, kterým lze též nastavit rozsvícení při narušení a tím zastrašit narušitele. Sloupky jsou z bezpečnostních důvodů dále osazeny tampery proti přelezení. Alternativou k IR závorám by mohly být zemní štěrbinové hadice i v provedení v dvojitém kabelu či optický vláknový systém. Další chráněnou částí byl plášť budovy, který je dle zvoleného stupně zabezpečení chráněn magnetickým kontakty na všech dveřích, oknech i garážových vratech. Dále je plášť chráněn detektory tříštění skla na kritických, velkých prosklených, částech budovy a okénko v garáži, kde se nachází cenný automobil. Dále jsou vnitřní prostory chráněny duálními PIR detektory pohybu pro případ, že by se narušitel dostal až do vnitřních prostor. Ty jsou dále kontrolovány stropními detektory kouře. Přístup do budovy je realizován u hlavních dveří biometrickým

elektronickým zámkem na otisk prstu či heslo doplnitelný o biometrickou kliku pro pohodlnější funkci. Přístup na pozemek je realizován brankou na mechanický klíč se zvonkem doplnitelnou o interkom či videointerkom a vzdáleným otevíráním dveří z pohodlí domova, vjezdová brána do garáže by pak mohla být též ovládána dálkově ovladačem. Alternativní možností k videointerkomu by byl klasický audio interkom doplněný o kameru, která by též mohla sloužit jako prvek PZS. Například IP kamera s detekcí pohybu či PTZ s nastavitelným natočením do pozice, odkud bylo zaznamenáno narušení. Pro záznam z kamery by bylo nutné systém dále doplnit o DVR. K ovládání systému by byly využity klávesnice uvnitř budovy navrhnuté u hlavních dveří, v/u garáže a v kuchyni vedle prosklených dveří na terasu. Ty jsem zvolil 3 různé typy dle umístění, u hlavních dveří a v kuchyni by byl schopné na půdorysu zobrazovat narušené zóny. Dále by byl systém ovladatelný pomocí dálkových ovladačů o dosahu až 70m, za tímto účelem je systém doplněn o bezdrátový obousměrně komunikující modul. V návrhu jsem zvolil i typ ústředny a to s možností až 4 podsystémů, jež by měly být dostačující. Díky nim lze snadno rozdělit a jednoduše ovládat jednotlivé prvky zabezpečení jako perimetr, plášť a interiér budovy dle patra. Počet zón by mohl stačit základní na desce ústředny, ale dle požadavků lze rozšířit expandérem o další a zóny rozlišit detailněji. Prvky jsem zvolil z valné většiny (až na hlásiče kouře) drátové, které jsou bezpečnější a méně náchylné na rušení, jejich rozvody bych navrhoval v plastových trubkách pod omítkou, prvky z prvního patra k ústředně v přízemí bych navrhl vést kolem potrubí odpadu či dle konstrukce domu ve zdi a vnější IR závory spolu s elektrickým vedením či potrubím dovnitř budovy v pancéřových trubkách, použity by byly více žilové SYKFY stíněné. Systém je dále vybaven jednou vnitřní sirénou na chodbě v přízemí a jednu vnější zálohovanou umístěnou na čelní straně domu v prvním patře. Dále je informace o stavu systému posílána na PCO a to s pomocí komunikačního modulu PCS300 IP protokolem přes internet, které by zaslalo na místo zásahový vůz a informovala majitele domu.

ZÁVĚR

Ve své bakalářské práci jsem se zaměřil na problematiku zajištění bezpečnosti pláště budov a to za pomoci moderních technologií, jako jsou kamerové systémy, přístupové systémy, detektory tříštění skla, otřesové detektory, kabely mikrofonní, štěrbinové, optické a další, a to za účelem zabezpečení objektu z hlediska zdraví a života osob a majetku.

V první kapitole teoretické části jsem se zaměřil na definici základní bezpečnostní terminologie, rozebral statistiku trestné činnosti vloupáním v ČR s využitím podkladů PČR, uvedl způsoby vniknutí do objektu, zmínil důležitost ochrany perimetru a jednotlivé fakta znázornil i graficky. V nejrozsáhlejší části práce jsem se věnoval jednotlivým technologiím zajišťujícím bezpečnost objektů, zde jsem nejčastěji uvedl základní teorii, princip jejich fungování, technické schopnosti a okrajově též zásady montáže těchto zařízení. V následující části jsem se již zabýval konkrétním materiálem dostupným na trhu v ČR a EU. Zde jsem nejdříve uvedl distributory zajišťující dodávku, montáž, zaškolení a servis bezpečnostních systémů a následně již konkrétní výrobce s bližším pohledem na jejich jednotlivé řady uváděné na trh a jejich základní funkce, technické vlastnosti, schopnosti. Následující kapitola byla věnována legislativě těchto zařízení a to zejména legislativě v ČR, jež se skládala z platných zákonů ČR upravující certifikaci, akreditaci a státní zkušebnictví, nařízení vlády a českých technických norem stanovující technické požadavky v oblasti PKB. Poslední kapitola teoretické části práce byla zaměřena na směr budoucího vývoje těchto technologií a prognózu, zde jsem uvedl trendy ve vývoji video techniky PKB, spojení mechaniky, elektroniky a strojírenství pod názvem mechatronika a její využití zejména v tzv. inteligentních budovách. Posledním tématem vývojových trendů byly přístupové systémy a to biometrické založené na principu ezoterické biometrie, tedy skrytých biometrických příznaků.

Praktická část této bakalářské práce je věnována návrhu bezpečnostního řešení pro jeden konkrétní fiktivní objekt, pro který byl vypracován popis a požadavky na projekt. Tato část dále obsahuje řešení konkrétního návrhu obsahující stanovení stupně zabezpečení, třídy prostředí a konkrétního návrhu použitých technologií včetně jejich rozmístění. Tento návrh je dále doplněn o konkrétní výrobky, jejich parametry, orientační cenovou kalkulaci a výpočty základního a náhradního napájecího zdroje.

CONCLUSION

In my thesis, I focused on the issues of security of building shells with the assistance of modern technologies such as CCTV, access control systems, glass break detectors, shock detectors, microphone cables, buried cables, optical and others, in order to security a facility in terms of human health and life and property.

In chapter one, I focused on the definition of basic security terminology, interpretation of the statistics of crime breaking-in in Czech Republic using police documents, introduced methods of intrusion into the building, mentioned the importance of protecting the perimeter and the individual facts depicted graphically. The largest part of the work I was paid to individual technologies to ensure the security of buildings, I have introduced here the basic theory, principles of operation, technical ability and also marginally installation principles of these devices. In the following section I have dealt with the specific materials available on the market in the Czech Republic and the European Union. Here, I first introduced the distributors providing delivery, installation, training and service of security systems and then a particular manufacturer with a closer look at their individual series placed on the market and their basic functions, technical features, capabilities. The following chapter was devoted to the legislation of these devices and particular legislation in the Czech Republic, which was made up from legislation regulating the certification, accreditation and state testing, and Government Order of the Czech technical standards specifying the technical requirements of Commercial Security. The last chapter of the work was focused on the future direction of technology development and prognosis, there I pointed the trends in video technology, Commercial Security, combination of mechanics, electronics and engineering as mechatronics and its use particularly in the so-called intelligent buildings. The latest theme of development trends has been access systems and biometric based on the principle of esoteric biometrics, biometric latent symptoms.

A practical part of this thesis is devoted to the design of security solutions for a specific imaginary object, for which was developed the description and requirements for the project. This part also includes solving a specific design contain choose of security level, class of environment and the specific technologies including their placement. This design is supplemented with specific products, their characteristics, orientation price calculation and calculations of main and secondary power sources.

SEZNAM POUŽITÉ LITERATURY

[1] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 3. aktualiz. S.l. : Cricetus, 2006. 313 s. ISBN 80-902938-2-4(brož.)

[2] KINDL, Jiří. *Projektování bezpečnostních systémů I.* 2. vyd. Zlín : Univerzita Tomáše Bati, 2007. 134 s. ISBN 978-80-7318-554-1.

[3] ZEMAN, Petr. *Česká bezpečnostní terminologie*. Brno : Masarykova univerzita , 2002. 186 s. ISBN 80-210-3037-2.

[4] IVANKA, Ján. *Systemizace bezpečnostního průmyslu I.* 3. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 123 s. ISBN 978-80-7318-850-4.

[5] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 3. Zlín : Univerzita Tomáše Bati ve Zlíně, 2010. 81 s. ISBN 978-80-7318-889-4.

[6] ČANDÍK, Marek. *Technické prostředky bezpečnostního průmyslu.* Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta technologická, Ústav elektrotechniky a měření, 2005. 117 s. ISBN 8073183285.

[7] ČANDÍK, Marek. *Objektová bezpečnost II.* Vyd. 1. Zlín : Univerzita Tomáše Bati, 2004. 100 s. ISBN 8073182173.

[8] UHLÁŘ, Jan. *Technická ochrana objektů.* Vyd. 1. Praha : Policejní akademie české republiky, 2005. 229 s. ISBN 80-7251-189-0.

[9] *Policie České republiky* [online]. 2010 [cit. 2011-04-15]. Dostupné z WWW: <http://policie.cz/>.

[10] *TZB-info* [online]. 2002 [cit. 2011-04-15]. Inteligentní budova. Dostupné z WWW: <http://www.tzb-info.cz/1143-inteligentni-budova-i>.

[11] *Úřad pro technickou normalizaci, metrologii a státní zkušebnictví* [online]. 2011 [cit. 2011-04-15]. Dostupné z WWW: <http://unmz.cz>.

[12] Zákon č. 22/1997 Sb. O technických požadavcích na výrobky a o změně a doplnění některých zákonů [cit. 2011-04-15]

[13] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi*. VŠB TU Ostrava, 2008. 58 s. Dostupné z WWW: <http://www.fbi.vsb.cz/miranda2/export/sites-root/fbi/040/cs/sys/resource/PDF/biometricke_metody.pdf>.

[14] *ADI Global Distribution* [online]. 2011 [cit. 2011-04-17]. Dostupné z WWW: <http://adiglobal.cz>

[15] *EUROALARM* [online]. 2007 [cit. 2011-04-29]. Dostupné z WWW: <http://euroalarm.cz/>.

[16] *EUROSAT CS* [online]. 2011 [cit. 2011-04-29]. Dostupné z WWW: <http://eurosat.cz/>.

[17] *STASANET* [online]. 2005 [cit. 2011-04-29]. Dostupné z WWW: <http://stasanet.cz/>.

[18] *SEGURO* [online]. 2009 [cit. 2011-04-29]. Dostupné z WWW: <http://seguro.cz/>.

[19] *MARCOMPLET* [online]. 2006 [cit. 2011-04-29]. Dostupné z WWW: <http://marcomplet.cz/>.

[20] *VIVOTEK* [online]. 2011 [cit. 2011-04-29]. Dostupné z WWW: <http://vivotek.cz/>.

[21] *AXIS COMMUNICATIONS* [online]. 2010 [cit. 2011-04-29]. Dostupné z WWW: <http://axis.com/>.

[22] *Arecont Vision* [online]. 2010 [cit. 2011-04-29]. Dostupné z WWW: <http://arecontvision.com/>.

[23] *Honeywell* [online]. 2011 [cit. 2011-04-29]. Dostupné z WWW: <http://honeywell.com/>.

[24] *SENSTAR* [online]. 2011 [cit. 2011-04-29]. Dostupné z WWW: <http://senstar.com/>.

[25] *Perimeterlarm* [online]. 2009 [cit. 2011-04-29]. Dostupné z WWW: <http://perimeterlarm.se/eng/>.

[26] *FiberPatrol by Optellios* [online]. 2011 [cit. 2011-04-29]. Dostupné z WWW: <http://fiberpatrol.com/>.

[27] *OPTEX* [online]. 2010 [cit. 2011-04-29]. Dostupné z WWW: <http://optexeurope.com>.

[28] *CoNet s.r.o.* [online]. 2011 [cit. 2011-04-29]. Dostupné z WWW: <http://conet.cz/>.

[29] *SOUTHWEST MICROWAVE* [online]. 2011 [cit. 2011-04-29]. Dostupné z WWW: <http://southwestmicrowave.com/>.

[30] IVANKA, Ján. *Mechanické zábranné systémy*. Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2010. 151 s. ISBN 978-80-7318-910-5.

[31] *VOKNO s.r.o.* [online]. 2010 [cit. 2011-05-05]. Dostupné z WWW: <http://vokno-plastova-okna.cz>.

[32] *Vše pro okna* [online]. 2010 [cit. 2011-05-05]. Statistika vloupání v Praze a v ČR. Dostupné z WWW: <http://www.vseprookna.cz/statistika-vloupani/>.

[33] *IP kamery a zařízení* [online]. 2011 [cit. 2011-05-05]. Dostupné z WWW: <http://netcam.cz/>.

[34] *HRG* [online]. [cit. 2011-05-07]. Ground Perimeter Security Systems. Dostupné z WWW: <http://homeresourceguide.com/MediaBuss-GPS.html>.

[35] *Perimeter Protection* [online]. 2011 [cit. 2011-05-07]. Perimeter Security Systems. Dostupné z WWW: <http://gforcesystems.com/products/perimter-protection/>.

[36] *Kriminalistika* [online]. 0 [cit. 2011-05-07]. Kriminalistická daktyloskopie. Dostupné z WWW: <http://kriminalistika.eu/daktyl/daktyl.html>.

[37] *Katalog-doktorů* [online]. 20.1.2010 [cit. 2011-05-07]. Lidské oko. Dostupné z WWW: <http://katalog-doktoru.cz/zajimavosti/32-lidske-oko/>.

[38] *Vysoká škola báňská - Technická univerzita Ostrava* [online]. 2010 [cit. 2011-05-07]. Dostupné z WWW: <http://www.vsb.cz/>.

[39] *PROJEKTY STAVEB - Luboš Purmenský* [online]. [cit. 2011-05-07]. Dostupné z WWW: <http://projekty-purmensky.cz/>.

[40] JABLOTRON ALARMS a.s.. Jablonec nad Nisou. *Podniková norma PNJ 131*. 2007. 20 s.

[41] *AUTOMA časopis pro automatizační techniku* [online]. 2010 [cit. 2011-05-07]. EMC v technické praxi I: Legislativní požadavky. Dostupné z WWW: <http://odbornecasopisy.cz/index.php?id_document=30967>.

[42] *JABLOTRON ALARMS a.s.* [online]. 2008 [cit. 2011-05-07]. Dostupné z WWW: <http://jablotron.cz>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Systémy řízení a kontroly vstupů.
EKV	Elektronická kontrola vstupu.
FAR	Koeficient nesprávného přijetí.
FRR	Koeficient nesprávného odmítnutí.
FER	Poměr osob, u kterých došlo k selhání procesu sejmutí příznaku.
FIR	Koeficient nesprávné identifikace.
FMR	Koeficient nesprávného rozpoznání.
FNMR	Koeficient nesprávné nerozpoznání.
TFT	Tenkovrstvý tranzistor.
CCD	Elektronická součástka pro snímání obrazové informace.
DNA	Deoxyribonukleová kyselina.
CMOS	Elektronická součástka pro snímání obrazové informace.
IR	Infračervené záření.
PIR	Pasivní infračervený detektor.
PZS	Poplachový zabezpečovací systém.
PZTS	Poplachový zabezpečovací a tísňový systém.
MZS	Mechanický zábranný systém.
MW	Mikrovlnný detektor.
US	Ultrazvukový detektor.
IP	Protokol pro komunikaci v počítačové síti.
FTP	Protokol pro přenos souborů v počítačové síti.
UTP	Nestíněná strukturovaná kabeláž.
AC	Střídavý proud.
DC	Stejnosměrný proud.

NVR	Videorekordér pro záznam z IP kamer.
PTZ	Polohovací kamera.
SW	Programové vybavení počítače.
HW	Hardwarové vybavení počítače.
HDD	Pevný disk
GPS	Zemní perimetrický systém (Zemní tlakové hadice).
CCTV	Uzavřený televizní okruh.
EPS	Elektronický požární systém
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.
ČNI	Český normalizační institut.
PCO	Pult centralizované ochrany.
PKB	Průmysl komerční bezpečnosti.
NBÚ	Národní bezpečnostní úřad.
NC	Kontakt Normal Open.
ATZ	Smyčka odporově vyvažovaná.
SS	Stejnosměrný proud.
PGM	Programovatelný výstup.
RC4	Kryptovací algoritmus.
MD5	Hash algoritmus.
AES	Symetrická bloková šifra.
GPRS	Mobilní datová služba.
LCD	Displej z tekutých krystalů.
MPx	MegaPixel – počet obrazových bodů.

SEZNAM OBRÁZKŮ

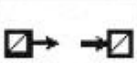
SEZNAM TABULEK

SEZNAM PŘÍLOH

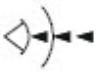
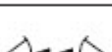
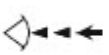
PŘÍLOHA P I: SCHEMATICKÉ ZNAČKY

Uvedené schematické značky jsou přejaté z podnikové normy PNJ 131 od firmy Jablotron.

Sch. značka dle ČSN 50131	Zjednodušená sch. značka	Popis prvku
		Výstražné zařízení maják
EZS	U	Ústředna EZS
		Napájecí zdroj
EXP		Expandér, link. modul koncentrátor
TAB		Tablo EZS
		Přenosové zařízení komunikátor
		Transformátor 220/16 V
		Záložní akumulátor
	UC	Přijímač řady UC (216, 220, ...)
		Expandér řady UC 280
		Detektor kouře

Sch. značka dle ČSN 50131	Zjednodušená sch. značka	Popis prvku
		Bezdrátový vysílač, přijímač
		Klíčový spínač
		Propouštěcí zámek
		Ovladač, klávesnice
		Vstupně-výstupní modul
REL		Reléový modul
		Detektor kouře
	GSM	Vysílač GSM
	PCO	Vysílač PCO
		Záplavový detektor
		Vývod kabelu

[40]

Sch. značka dle ČSN 50131	Zjednodušená sch. značka	Popis prvku
		Magnetický detektor
		Magnetický detektor - odolný
		Detektor tříštění skla
		Detektor tříštění skla - antimasking
		Kontaktní detektor piezo
		PIR vějíř
		PIR vějíř venkovní
		PIR vějíř antimasking
		PIR dlouhý dosah
		PIR s vlastní adresou
		PIR záclona
		PIR záclona antimasking
		PIR záclona dveřní
		Infrazávora
		Infrazávora vysílač
		Infrazávora přijímač
		Ultrazvukový detektor
		PIR stropní

Sch. značka dle ČSN 50131	Zjednodušená sch. značka	Popis prvku
		Kombinovaný detektor PIR strpní a GBS
		**Kombinovaný detektor PIR a GBS (JS-25)**
		Mikrovlnný detektor
		Duální detektor mikrovlna, PIR
		Duální stropní detek. mikrovlna, PIR
		Otřesový detektor
		Detektor poslední bankovky
		Tísňový hlásič PANIC tlačítko
		Tísňový hlásič PANIC lišta
		Technologický hlásič
		Detektor hořlavých plynů
		Požární hlásič
		Signalizace optická
		Signalizace optická a akustická
		Vnitřní siréna s blikačem
		Vnitřní siréna
		Venkovní siréna s blikačem
		Venkovní siréna

PŘÍLOHA P II: PŘIBLIŽNÁ CENOVÁ KALKULACE NÁVRHU

Zařízení	Popis	Cena vč. DPH [Kč]	Počet kusů	Cena celkem [Kč]
EVO48	PZS ústředna PARADOX	2639	1	2639
PCS300/IP	Internetový TCP/IP modul PARADOX	3550	1	3550
APR-ZX8	Sběrnicový rozšiřující modul 8 zón (16 ATZ)	1443	1	1443
RTX3-433/868	Bezdrátový obousměrný přijímač a vysílač	2179	1	2179
AX-130TN	Vnější infrazávora OPTEX, dosah 40m exteriér	4428	12	53136
MALTA	Jednostranný sloup s výškou 2m a možností směrování infrazávor v rozsahu 180°	9903	4	39612
BUNKER TAE	Tamper proti přelezení sloupu	1901	4	7604
USP500SP	Průmyslový magnetický kontakt, polarizovaný, opancéřované drátové vývody	863	2	1726
USP3000SP	Magnetický kontakt - vratový	421	1	421
USP-A1DW	Závrtný magnetický kontakt	78	16	1248
GLASSTREK DG457	Sběrnicový detektor tříštění skla PARADOX	2399	4	9596
DGP2-50	Sběrnicový IR detektor s duálním senzorem, BUS IMPERIAL/EVO	740	9	6660
MG-SD738	Bezdrátový optický detektor kouře	2220	2	4440
TM4	Dotyková barevná grafická LCD sběrnicová klávesnice	7990	1	7990
GRAFICA COLOR LCD	Barevná grafická LCD sběrnicová klávesnice s teploměrem	6990	1	6990
K656	Dotyková LCD klávesnice s modrým podsvitem	2999	1	2999
PS-128 SIGNAL	Venkovní zálohovaná siréna PARADOX	1429	1	1429
SA-105	piezosiréna 120dB	259	1	259
Biocav HDBFD-1000	Biometrický elektronický zámek	8982	1	8982
MG-REM2	Šestipovelvý bezdrátový ovladač 433/868MHz s obousměrnou komunikací	1330	5	6650
SYKFY 4x2x0,5	Stíněný kabel pro zabezpečovací techniku	10	550	5280
TP-12180	Záložní bezúdržbový akumulátor kapacity 18Ah	1160	1	1160
TP-1213	Záložní bezúdržbový akumulátor kapacity 1,3Ah	269	1	269
Cena celkem vč. DPH				176 262 Kč

Uvedené ceny jsou pouze orientační, mohou se lišit v závislosti na dodavateli, dále také v celkové ceně nejsou započteny všechny ostatní doplňující komponenty a cena práce, která bude stát dalších několik desítek tisíc Kč.

PŘÍLOHA P III: VÝPOČET ZDROJŮ

Zařízení	Odběr v klidu [mA]	odběr v poplachu [mA]	Počet kusů	Celkem v klidu [mA]	Celkem v poplachu [mA]
EVO48	100	200	1	100	200
PCS300/IP	150	250	1	150	250
APR-ZX8	28	28	1	28	28
RTX3-433/868	120	140	1	120	140
AX-130TN	41	200	12	492	2400
USP500SP	0	0	2	0	0
USP3000SP	0	0	1	0	0
USP-A1DW	0	0	16	0	0
GLASSTREK DG457	25	25	4	100	100
DGP2-50	15	15	9	135	135
TM4	70	110	1	70	110
GRAFICA COLOR LCD	90	130	1	90	130
K656	80	120	1	80	120
PS-128 SIGNAL	5	2800	1	5	2800
SA-105	5	250	1	5	250
Celkem [mA]				1375	6663

Výpočet kapacity základního zdroje

1,375A . 12h = 16,5 Ah > Orientačně volím vyšší 18Ah

Dobíjecí proud akumulátoru

16,5 Ah . 0,8 = 14,4 Ah : 72 h = 0,2A

1,375A + 0,2A = 1,575A

Výkon základního zdroje

13,8V . 1,5757A = 21,735 VA

Výpočet kapacity záložního akumulátoru

KNZ = (12 – 0,25) . 1,375 + 0,25 . 6,663 = 17,882 Ah > Akumulátor typu A 18Ah

$$T = \frac{17{,}882 + 0{,}25.1{,}375 - 0{,}25.6{,}663}{1{,}375} = 12h$$

Výpočet kapacity záložního akumulátoru venkovní sirény

KNZ = (12 – 0,25) . 0,005 + 0,25 . 2,8 = 0,75875 Ah > Akumulátor typu A 1,3Ah

$$T = \frac{0{,}75875 + 0{,}25.0{,}005 - 0{,}25.2{,}8}{0{,}005} = 36{,}75h$$