Objektová bezpečnosť a režimové opatrenia

Building security and regime's actions

Monika Hanzenová

Bakalárska práca
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:	**Monika HANZENOVÁ**
Osobní číslo:	**A08117**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Objektová bezpečnost a režimová opatření**

Zásady pro vypracování:

1. **Popište správné zajištění objektové bezpečnosti z technického hlediska a navrhněte účinná režimová opatření pro vzorové použití**
2. **Vyjádřete současný stav objektové bezpečnosti v Slovenské republice a zranitelnost objektů.**
3. **Popište takticko-technické návrhy na zefektivnění objektové bezpečnosti.**
4. **Proveďte analýzu zranitelnosti objektu.**
5. **Předložte návrhy aktivních režimových opatření v průmyslových areálech a velkých střežených objektech.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BRABEC, F.: Ochrana bezpečnosti podniku. Eurounion, Praha 1996, ISBN 80-85858-29-0.**
2. **BRABEC, F. a kol. Hlídací služby. Eurounion, Praha 1995, ISBN 80-85858-12-6.**
3. **LÁTAL, I. a kol. Bezpečnostní zásady ochrany podniku. Prospektrum, Praha 2001,**
4. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. UTB Zlín, 2010, ISBN 978-80-7318-889-4.**
5. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. UTB Zlín, 2007, ISBN 978-80-7318-631-9.**
6. **LAUCKÝ, Vladimír. Řízení technologických procesú v průmyslu komerční bezpečnosti. UTB Zlín, 2006, ISBN 80-7318-432-X.**
7. **HURTA, J., LAUCKÝ, V. Management bezpečnostního inženýrství. UTB Zlín FAI, 2006, ISBN 80-7318-412-5.**
8. **KAMENÍK, J., BRABEC, František a kol. Komerční bezpečnost. ASPI Wolters Kluwer, Praha 2007, ISBN 978-80-7357-309-6.**

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

Cieľom bakalárskej práce je popísanie správneho zaistenia objektovej bezpečnosti z technického hľadiska a návrh účinných režimových opatrení. Práca sa snaží vyjadriť súčasný stav objektovej bezpečnosti v Slovenskej republike a stručne popísať takticko – technické návrhy na zefektívnenie bezpečnosti objektov. V praktickej časti sú navrhnuté účinné režimové opatrenia fiktívnej firmy pre takzvané vzorové použitie.

K vypracovaniu bakalárskej práce bola použitá odborná literatúra týkajúca sa danej problematiky.

Kľúčové slová:

Objektová bezpečnosť, fyzická bezpečnosť, technická bezpečnosť, režimové opatrenia, zraniteľnosť objektu, bezpečnostná politika,

ABSTRACT

The aim of bachelor work is to describe the correct ensure of object safety from a technical standpoint and proposal of effective regime measure. Work tries to express the current state of building security in the Slovak Republic and briefly describe the tactical and technical proposals to streamlining the safety of objects. In the practical part of the work are proposed effective regime measures of fictional company as model for using.

For elaboration bachelors work was used specialist literature concerning the issue.

Keywords:

Building security, physical security, technical security, regime measures, vulnerability of building, security policy,

Týmto by som chcela poďakovať JUDr. Vladimírovi Lauckému, za jeho láskavý prístup a podporu, odborné vedenie, ochotne poskytnutý čas a cenné rady, ktoré mi venoval pri vypracovaní mojej bakalárskej práce. Tiež by som sa chcela poďakovať Ing. Ladislavovi Hanzenovi za odborné konzultácie na danú tému.

Motto: „Bezpečnosť je len taká silná, ako je jej najslabší článok“

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

Fyzická a objektová bezpečnosť je súbor opatrení, ktoré slúžia na ochranu utajovaných skutočností pred odcudzením a neoprávnenou manipuláciou v chránených priestoroch a objektoch. Vzhľadom k stále rozšírenejšiemu rozmachu rôznych druhov kriminality je otázka zabezpečenia svojho majetku na prvom mieste.

Ochrana je súhrn činností, ktoré musíme realizovať aby sme odvrátili alebo zmiernili následky vznikajúce neoprávneným vstupom do chráneného priestoru. Ochrana objektu nie je len komplex technickej a fyzickej ochrany. Základom zaistenia dokonalej ochrany podniku je spôsob správania sa zamestnancov, ľudí nachádzajúcich sa v objekte, podľa stanovených pravidiel, zásad, noriem, zakotvených v režimových opatreniach a bezpečnostnej politiky podniku. V dnešnej dobe musí majiteľ objektu dbať na to, aby bola ochrana objektu vykonávaná na základe najnovších technológií zabezpečovacích systémov, musí dbať na ich inováciu a pružnosť. Integrovanie systémov je jednou z možností ako dosiahnuť lepších výsledkov v zabezpečení objektu.

Hlavnou myšlienkou, na ktorú by každý majiteľ pri zaisťovaní bezpečnosti súkromného objektu alebo podniku mal myslieť je, že každý narušiteľ, páchateľ, pokiaľ má dôvod sa do objektu dostane, rozhodujúci je čas, ktorý je na to potrebný. V najlepšom možnom prípade by tento čas mal byť minimálne aspoň rovnaký s časom, ktorý trvá zásahovej službe, alebo majiteľovi dostať sa k objektu od chvíle prvej signalizácie narušenia objektu.

Cieľom mojej bakalárskej práce je popísanie správneho zaistenia objektovej bezpečnosti z technického hľadiska a navrhnutie účinných režimových opatrení veľkých priemyselných areálov pre vzorové použitie. Téma práce stelesňuje základný prvotný návod na ochranu podnikov od technických prvkov až po vnútropodnikové smernice, či nariadenia.

Teoretická časť rieši problematiku technickej a legislatívnej podpory na ochranu strážených priestorov a takticko – technické návrhy na zvýšenie, zefektívnenie požadovanej bezpečnosti v podobe integrovaných systémov bezpečnosti. Ťažiskom práce je analýza zraniteľnosti objektu, ktorá vytvára základ pre vytvorenie systému ochrany objektu. Od nej sa ďalej odvíja vypracovanie dokumentov bezpečnostného projektu a bezpečnostnej politiky podniku.

Praktická časť poukazuje a stručne popisuje súčasný stav objektovej bezpečnosti v SR. Piata kapitola slúži ako návod aktívnych režimových opatrení slúžiacich na zaistenie bezpečnosti vo fiktívnej firme.

I. TEORETICKÁ ČASŤ

1 SPRÁVNE ZAISTENIE OBEJKTOVEJ BEZPEČNOSTI Z TECHNICKÉHO HĽADISKA

1.1 Prehľad platnej legislatívy využívanej pri realizácii chránených priestorov

Právne predpisy:

- Vyhláška NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení vyhlášky NBÚ č. 315/2006 Z. z,
- Vyhláška NBÚ č. 314/2006 Z. z., ktorou sa mení a dopĺňa vyhláška NBÚ č. 337/2004Z. z., ktorou sa upravujú podrobnosti o certifikácií mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní,
- Zákon NR SR č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.

Technické predpisy:

- STN EN 50131-1 Poplachové systémy. Elektrické zabezpečovacie systémy. Časť 1Všeobecné požiadavky,
- STN EN 50 132-2-1 Poplachové systémy. Sledovacie systémy CCTV na používanie v bezpečnostných aplikáciách. Čiernobiele kamery,
- STN EN 50133-1 Poplachové systémy. Systémy kontroly vstupov na používanie v bezpečnostných aplikáciách. Požiadavky na systém,
- STN P ENV 1627 Okná, dvere, uzávery. Odolnosť proti vlámaniu. Požiadavky a triedenie,
- STN P ENV 1303 Stavebné kovanie. Cylindrické vložky do zámok. Požiadavky a skúšobné metódy,
- STN P ENV 1906 Stavebné kovanie. Dverové kľučky a gule. Požiadavky a skúšobné metódy,
- STN EN 356 Sklo v stavebníctve. Bezpečnostné zasklenie. Skúšanie a klasifikácia odolnosti proti ručnému útoku,
- STN EN 12209 Stavebné kovanie. Zámky a uzávery. Mechanicky ovládané zámky, uzávery a zapadacie plechy. Požiadavky a skúšobné metódy,

- STN EN 334590 Elektrotechnické predpisy. Zariadenia elektrickej zabezpečovacej signalizácie,
- STN 1143 - 1 Bezpečnostné úschovné objekty. Požiadavky, klasifikácia a metódy skúšania odolnosti proti vlámaniu. Časť 1: Skriňové trezory, trezorové dvere a komorové trezory,
- STN 369510-1 Kancelárske stroje. Deštrukcia nosičov informácií. Časť 1: Požiadavky na skúšobné metódy na zariadenia a inštaláciu.

1.2 Objektová bezpečnosť

Ochrana majetku podnikateľských aj fyzických subjektov pred protiprávnym jednaním, je témou, ktorá v priebehu posledných rokov silno získava na význame.

Objekt je budova, alebo iný stavebný priestor, kde sa nachádzajú priestory, ktoré chceme chrániť.

Bezpečnosť rozumieme ako stav štátu, kedy sa zachovávajú demokratické základy, vnútorná bezpečnosť, suverenita a poriadok a stav, kedy je chránené životné prostredie.

„*Fyzická bezpečnosť a objektová bezpečnosť je systém opatrení slúžiaci na ochranu utajovaných skutočností pred nepovolanými osobami a pred neoprávnenou manipuláciou v objektoch a chránených priestoroch*.“(Ing. Tomáš LOVEČEK, 2006),

Objektová bezpečnosť je zdĺhavý proces, ktorým sa zaisťuje personálne a technické zaistenie zabezpečenia objektu tak, aby akékoľvek narušenie, ukradnutie utajovanej skutočnosti bolo eliminované na minimum. Vo všeobecnosti ide o vytvorenie bezpečného prostredia pre daný subjekt. Pre návrh konkrétnej ochrany musíme poznať predmet a cieľ ochrany. Realizácia objektovej ochrany predstavuje návrh a zladenie všetkých dostupných prostriedkov, ktoré sú schopné zaistiť požadovanú bezpečnosť. [4]

Bezpečnosť je zaisťovaná :

- fyzickou ochranou,
- technickou ochranou,
  - mechanická,
  - elektronická,
  - režimové opatrenia,

- špeciálna ochrana,
- kombinovanou ochranou.

Bezpečnostný systém zaisťuje:

- osobnú bezpečnosť,
- informačnú bezpečnosť,
- majetkovú bezpečnosť.

Z priestorového hľadiska delíme ochranu objektu:

- obvodovú,[1]
- plášťovú,
- priestorovú,
- predmetovú.

Pri navrhovaní ochrany platia tri základné pravidlá:

- žiadna absolútna ochrana neexistuje => každá ochrana môže byť prekonaná,
- jedna skupina ochrany nestačí,
- technické prostriedky nemôžu úplne nahradiť človeka =>človek musí vyhodnotiť, či je nahlásené narušenie skutočné a podniknúť adekvátne kroky. [3], [6], [10]

1.3 Spôsoby zaistenia ochrany objektu

Ochrana objektu je veľmi dôležitým úkonom, ktorý môže byť zaistený rôznymi spôsobmi.

- fyzickou ochranou,
- technickou ochranou,
  - mechanické zábranné prostriedky,
  - elektronické prostriedky,
- režimovou ochranou.

[1]perimetrickú

1.3.1 Fyzická ochrana

Podľa zákonu 336/2004 § 9: *Fyzickú ochranu objektu a chráneného priestoru (ďalej len "fyzická ochrana") vykonávajú príslušníci ozbrojených síl, ozbrojených bezpečnostných zborov, bezpečnostných zborov, zamestnanci súkromných bezpečnostných služieb, zamestnanci prevádzkovateľa objektu alebo vlastní zamestnanci*."

Fyzická ochrana jenajstaršou a najčastejšou formou zaisťovania a ochrany majetku a osôb, ktorá je vykonávaná „živou silou". Pracovník fyzickej ostrahy, ako jediný druh ochrany je v prípade nutnosti schopný vykonať zákrok k odvráteniu hroziaceho nebezpečenstva. Tím sa aktívne podieľa na dolapení páchateľa. Aktívny zásah je jednou z najväčších predností ochrany vykonávanej fyzickou osobou, čím môžeme odvrátiť hroziace nebezpečenstvo, alebo aspoň znížiť rozsah škody na minimum. Ďalšími prednosťami použitia fyzického pracovníka, sú rozsah jeho skúseností, znalostí, ktoré sa ďalej môžu vyvíjať, trvalá prítomnosť v objekte, tiež možnosť využitia pri živelných pohromách. Ide o ochranu vykonávanú príslušníkmi ozbrojených zborov, pracovníkmi súkromných bezpečnostných služieb, strážnikom, vrátnikom, alebo políciou. Po finančnej stránke je to najdrahšia metóda zaistenia ochrany objektu, ktorá vyžaduje pravidelný prísun peňazí vo forme mzdy, po celú dobu zaisťovania ochrany. Na rozdiel od technických zabezpečovacích prvkov, ktoré potrebujú iba jednorazovú vstupnú investíciu. Pracovníci fyzickej ostrahy plnia rôzne úlohy:

- kontrola vstupu a vjazdu,
- recepčná služba,
- poštovná a faxová služba,
- obchôdzky.

Fyzickú ochranu môžeme rozdeliť podľa rôznych kritérií.

- Časové kritérium,
  - fyzická ochrana vykonávaná len v pracovnej dobe,
  - fyzická ochrana vykonávaná nepretržito 24 hodín denne,
  - fyzická ochrana nárazová, vykonávaná podľa potrieb majiteľa.
- kritérium spôsobu zaistenia,
  - vlastní pracovníci fyzickej ostrahy,
  - prenajímaní pracovníci fyzickej ostrahy,
  - kombinácia pracovníci fyzickej ostrahy.

- kritérium rozsahu výkonu,
  - stacionárna fyzická ochrana,
  - obvodová fyzická ochrana,
  - dohľadová, celoplošná fyzická ochrana,
  - sprievodná fyzická ochrana,
  - dozorná fyzická ochrana,
  - zásahová fyzická ochrana,
  - revírna fyzická ochrana.
- kritérium výzbroje a výstroja,
  - ozbrojená fyzická ochrana,
  - neozbrojená fyzická ochrana,
  - verejná fyzická ochrana,
  - skrytá fyzická ochrana. [3],[6], [10]

1.3.2 Technická ochrana

Technická ochrana je súbor systémov, prvkov a komponentov, pomocou ktorých sa vytvárajú stále, nepretržité, bezpečnostné podmienky na ochranu objektu. Vďaka ním je zabránený vstup nepovolaným osobám do chráneného priestoru a zaistená signalizácia nepriaznivých, rizikových stavov, ktoré by mohli viesť k narušeniu zabezpečovaného objektu. Technická ochrana predstavuje najviac spoľahlivú ochranu, ktorá je ťažko prekonateľná. Cieľom technickej ochrany je zaistiť rýchle, nepretržité stráženie a monitorovanie chráneného objektu. Podľa zákona 336/2004 §4 sa za technické zabezpečovacie prostriedky považujú:

„a) systémy na kontrolu vstupov do objektov a systémy slúžiace na elektronické preukazovanie totožnosti a oprávnenosti osôb,

b) elektrické zabezpečovacie systémy (poplachové systémy na hlásenie narušenia),

c) kamerová zostava v rámci uzatvoreného televízneho okruhu,

d) tiesňové systémy,

e) zariadenia na detekciu látok a predmetov,

zariadenia fyzického ničenia nosičov informácií.“ [2], [5], [6]

1.3.3 Mechanické zábranné prostriedky

Mechanickým zábranným prostriedkom rozumieme prvok, komponent, ktorý svojou konštrukciou znemožňuje prekonanie a tým vniknutie do objektu. Úlohou mechanických zábranných systémov je páchateľovi znemožniť, sťažiť, zamedziť vniknutie do chráneného priestoru, prípadne zabrániť neoprávnenej manipulácií s predmetmi nachádzajúcimi sa v chránenom priestore. Do mechanickej ochrany radíme mechanické zábranné systémy obvodovej, plášťovej a predmetovej ochrany. Prvky mechanických zábranných systémov obvodovej ochrany sú všetky klasické a bezpečnostné oplotenia, brány, bránky, závory, vrcholové zábrany, hrebeňové bariéry, spomaľovacie zábrany, prejazdové retardéry, prekážky, turnikety a iné zábrany sťažujúce vniknutie do priestoru. Podľa zákona 336/2004 § 4 sa za mechanické zábranné prostriedky považujú:

„a) bezpečnostné úschovné objekty,

b) uzamykacie systémy a ich súčasti,

c) dvere a ich súčasti,

d) mreže,

e) bezpečnostné fólie,

f) okná,

g) zasklenia.“ [2], [5], [6]

Obrázok 1 Oplotenie ostnatým drôtom

Obrázok 2 Mreže

1.3.4 Elektronické prvky bezpečnosti

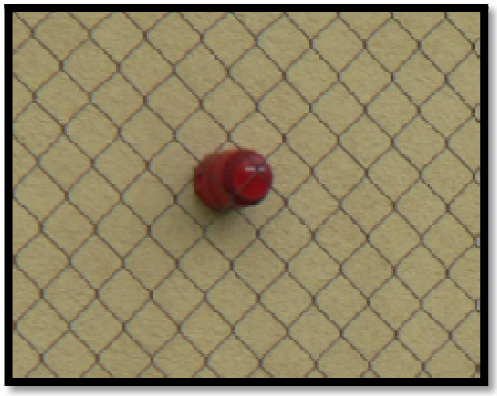
Elektronická ochrana, je typ zisťovania bezpečnosti pomocou elektronických a elektrických prvkov, ktorých úlohou je prevencia, informovanosť a dokumentovanie. Úloha prevencie je veľmi účinný a nevyhnutný spôsob ako zabrániť nekalým úmyslom páchateľa. Elektronický bezpečnostný systém je jednorazová investícia, ktorá nahradzuje alebo napomáha fyzickej ochrane. Ponúka nám možnosť informovania on-line o stave zabezpečovaných priestorov. Elektronické prvky ochrany treba umiestniť na viditeľnom mieste. Ak uvidí páchateľ, že je objekt strážený kamerovým systémom, spravidla si vyberie iný cieľ narušenia. K takémuto účelu slúžia aj atrapy, ktoré nie sú rozoznateľné od originálu. Úloha informovať, je tiež nevyhnutnou súčasťou. Elektronické prvky bezpečnosti, dokážu signalizovať miesto narušenia, čím zjednodušia a zrýchlia postup činnosti k zamedzeniu narušenia neoprávneným páchateľom a tiež dokumentovať situáciu, čím môžu napomôcť k dolapeniu páchateľa.

Medzi technické elektronické prvky patrí hlavne:

- elektrická zabezpečovacia signalizácia,
- elektrická požiarna signalizácia,
- prístupové a dochádzkové systémy,
- uzavreté strážiace a dohliadacie televízne okruhy,
- biometrické identifikačné systémy,
- satelitné vyhľadávanie vozidiel,
- ochrana dát a informácií,
- elektronická ochrana tovaru,

- priemyslová havarijná signalizácia. [2], [3], [5], [6], [10]

Obrázok 3 Bezpečnostná kamera



Obrázok 4 Signalizačné zariadenie

Obrázok 5 Pasívny infračervený detektor

1.3.5 Režimové opatrenia

Režimové opatrenia sú bezpečnostné smernice, ktoré prostredníctvom zavedených systémov opatrení zaistia ochranu majetku, osôb a iných bezpečnostných záujmov. Ide o súbor organizačne – administratívnych opatrení, ktoré majú predchádzať nežiaducim jednaním osôb nachádzajúcich sa v chránenom objekte a zaistiť správne fungovanie zabezpečovacieho systému a jeho zladenie s prevádzkou chráneného objektu.

Režimové opatrenia delíme na:

- Vonkajšie režimové opatrenia – zaisťujú hlavne vstupné a výstupné priestory chráneného objektu. Ide predovšetkým o vchody pre osoby, vjazdy pre automobily a iné vstupné brány. Tu dochádza ku kontrole osôb, vozidiel a vecí nachádzajúcich sa vo vozidle,
- Vnútorné režimové opatrenia – zaistenie sa týka vnútorných priestorov zabezpečovaného objektu. Najčastejšie ide o obmedzenie pohybu osôb alebo vozidiel priamo v objekte. Tiež sa vnútorné režimové opatrenia môžu týkať monitorovania pohybu materiálu a výrobkov, či zaistenia osvetlenia v určitých častiach objektu.

Na zabezpečenie týchto opatrení sú dôležité nasledujúce aspekty:

- vstupný a výstupný režim osôb a motorových vozidiel,
- materiálový a expedičný režim, ktorý zabraňuje rozkrádaniu majetku kontrolou prepravy evidovaného materiálu,
- prevádzkový režim, ktorého cieľom je zaistiť plynulosť a bezpečnosť prevádzky,
- kľúčový režim, kde ide hlavne o priraďovanie a odovzdávanie kľúčov, výmenu zámkov a pečatenie dverí alebo iných strážených častí objektu.

Základné pravidlá pre dodržiavanie režimových a organizačných opatrení:

- školenia zamestnancov,
- vytváranie bezpečnostného povedomia zamestnancov,
- články v rámci partnerských a pracovných zmlúv,
- vytváranie bezpečnostnej dokumentácie.

Podľa zákona 336/2004 § 10 medzi režimové opatrenia radíme opatrenia:

a) *„určujúce podmienky vstupu osôb a vjazdu dopravných prostriedkov do objektu a chráneného priestoru a podmienky výstupu osôb a výjazdu dopravných prostriedkov z objektu a chráneného priestoru,*
b) *určujúce podmienky pohybu osôb, dopravných prostriedkov v objekte a v chránenom priestore, a to v pracovnom čase a mimopracovnom čase,*
c) *určujúce podmienky používania mobilných telefónov, videokamier, fotoaparátov, audiozáznamových zariadení a podobne,*
d) *určujúce podmienky ochrany priestorov, kde sa utajované skutočnosti spracovávajú, rozmnožujú a ničia,*
e) *určujúce podmienky a spôsob kontroly objektu a chráneného priestoru po opustení pracoviska zamestnancami, ktoré zabezpečia, že nedôjde k neoprávnenej manipulácii s utajovanými skutočnosťami,*
f) *na ochranu rokovacích miestností,*
g) *určujúce podmienky používania, prideľovania, označovania, úschovy a evidencie originálov a kópií bezpečnostných kľúčov a médií do zámkov a uzamykateľných systémov,*
h) *určujúce podmienky používania, prideľovania, označovania, úschovy a evidencie kódových nastavení a hesiel používaných na prístup do objektov, chránených priestorov a bezpečnostných úschovných objektov,*
i) *určujúce podmienky manipulácie s mechanickými zábrannými prostriedkami a technickými zabezpečovacími prostriedkami a podmienky ich používania,*
j) *určujúce postup pri narušení objektu a chráneného priestoru alebo pri pokuse o narušenie objektu a chráneného priestoru,*
k) *určujúce postup v prípade vzniku mimoriadnej situácie, ktorých súčasťou je aj plán na ochranu, evakuáciu alebo zničenie utajovaných skutočností spolu s uvedením zodpovedných osôb; ak bezprostredne hrozí vznik mimoriadnej situácie alebo ak mimoriadna situácia už nastala, je vedúci oprávnený povoliť vstup do objektu alebo chráneného priestoru osobám zabezpečujúcim alebo vykonávajúcim záchranné akcie; v takých prípadoch pred vykonaním záchrannej akcie, v jej priebehu a bezprostredne po jej skončení musia byť prijaté opatrenia, ktoré zabránia úniku utajovaných skutočností.“* [1], [5]

Obrázok 6 Vstup do objektu na heslo

Obrázok 7 Režimové opatrenie

1.3.5.1 Základné dokumenty režimovej ochrany

Dodržiavanie režimových opatrení vo vnútri podniku si vyžaduje vypracovanie rôznych dokumentov režimovej ochrany. Podľa dôležitosti právnych noriem, ktoré riešia problematiku režimovej ochrany, je na prvom mieste štatút organizácie. Dokument, v ktorom je vyjadrená činnosť, cieľ a účel organizácie a dôležitosť jej postavenia. Na druhom mieste je organizačný poriadok zahrňujúci zmienku o stave ochrany podniku. Hovorí o štruktúre podniku, jeho jednotlivých častí a o prevádzkovej činnosti podniku.

Pracovný poriadok popisuje pracovné postupy, náplne pracovníkov, ich práva a povinnosti. Dôležitým dokumentom je spisovný poriadok, regulujúci informácie a pohyb spisovej agendy v podniku. V tomto dokumente by mali byť zahrnuté zásady obehu dokumentov. To znamená ich manipulácia, preprava, kopírovanie, ukladanie, systém ich posudzovania a schvaľovania a v neposlednom rade by mal obsahovať postupy v prípade strát. Spisový rád by mal tiež obsahovať manipulácie s kancelárskymi pomôckami. Ďalší dokument dôležitý pre vykonávanie režimovej ochrany je skartačný poriadok, ktorý určuje skartačné lehoty, metódy triedenia spisovej agendy či spôsob likvidácie spisov. V objektoch, kde sa využíva strážna služba, je potrebné vypracovať smernice strážnej služby.

[9]

1.3.6 Špeciálna ochrana

Spôsob ochrany, kde sa využívajú špeciálne prostriedky k zaisteniu ochrany jednotlivca, alebo predmetov nachádzajúcich sa v objekte. Tento typ ochrany obsahuje individuálne technické prostriedky a chemickú a fyzikálnu ochranu predmetov a dokumentov.

Tento typ ochrany v sebe zahŕňa prostriedky na ochranu jednotlivca akými sú – obranné spreje, paralyzéry, plynové a akustické pištole, osobné alarmy, intenzívne svetelné či bezpečnostné batožiny a prostriedky na ochranu predmetov a dokumentov, kam patrí napríklad – plomby, pečate, hologramy, chemické nástrahy a veľa ďalších. [9], [3]

Obrázok 8 Slzný sprej

1.4 Ochrana objektu z priestorového hľadiska

Ako som už spomínala, zaistenie bezpečnosti priestoru môžeme rozdeliť ako ochranu:

- perimetru,
- plášťa,
- priestoru,
- predmetu.

Na takúto ochranu nám slúžia okrem mechanických zábranných systémov aj detektory patriace medzi elektronický spôsob ochrany.

1.4.1 Detektory plášťovej ochrany

Prvky plášťovej ochrany tvoria dôležitú časť ochrany majetku. Ich úlohou je včas zachytiť a signalizovať pokus páchateľa o prekonanie klasickej ochrany objektu, akými sú všetky vonkajšie otvorové výplne, ale aj stavebné prvky budov akými sú steny, stropy, podlahy a strechy.

Detektory plášťovej ochrany:

- kontaktné,
- deštrukčné,
- detektory deštrukčných prejavov,
- bariérové,
- tlakové akustické.

1.4.1.1 Kontaktné detektory

Už sám názov nám napovedá, že kontaktné detektory, sú detektory, ktoré sú v priamom kontakte so stráženou plochou. Sú určitou konštrukčnou variantov kontaktu, ktorý je vrazený do zabezpečovacej slučky. Princíp spočíva v prerušení, alebo uzavretí prúdového okruhu zabezpečovacej slučky. Zabezpečovacou slučkou neustále preteká kľudový prúd, ktorý nepretržito kontroluje zabezpečovacia ústredňa. Poplach je vyhlásený v prípade, ak sa tento kľudový prúd zmení alebo preruší. Najčastejšie sa umiestňujú na miesta, aby bolo detekované otvorenie dverí, či okien do vzdialenosti maximálne 30 mm. [7]

Druhy kontaktných detektorov:

- mikrospínače,

dverné a prechodové kontakty,

- šmykové kontakty,
- nášľapné kontakty,
- nášľapné koberce,
- rozperné tyče,
- magnetické kontakty,
- závesné kontakty,
- koncové spínače.

1.4.1.2 Deštrukčné detektory

Sú to detektory, ktoré odvodzujú svoju funkciu od rozbitia fyzickej prekážky, ktorú musí narušiteľ prekonať. Ich hlavnou charakteristikou je nevratná funkcia, kedy pri detekcii narušenia sa zničia a stanú sa nepoužiteľnými, je potreba ich vymeniť, alebo opraviť.

Druhy deštrukčných detektorov:

- poplachové fólie, tapety a poplachové sklá,
- fóliové polepy,
- vodičové siete a zátarasy,
- svetlovodné zábranné siete.

1.4.1.3 Detektory deštruktívnych prejavov

Táto skupina prvkov plášťovej ochrany reaguje na otrasy, vibrácie, ktoré vznikajú pri pokusoch o narušenie chránených plôch.

Do skupiny detektorov deštruktívnych prejavov patria:

- otrasové detektory s mechanickým meničom,
- otrasové detektory s akusticky – elektrickým meničom,
- detektory na ochranu sklenených plôch,
- mikrofóne káble, [7]

- mechanické zábrany s detekciou narušenia.

1.4.1.4 Tlakové akustické detektory

Infrazvukový tlakový detektor využíva citlivý snímač a zosilňovač akustických frekvencií, ktoré vznikajú pri pohybe veľkých plôch alebo pri zmene objemových charakteristík chráneného priestoru. Infračervené detektory využívajú vynikajúcich vlastností v dobre utesnených objektoch v rodinných alebo tehlových domoch. Hlavnou výhodou tohto druhu detekcie, je ľahká inštalácia bez montáže vedenia a fakt, že stačí jeden detektor na celý objekt.

1.4.1.5 Bariérové detektory

Bariérové detektory slúžia k vytvoreniu umelej bariéry v strážených priestoroch. Vyžívajú na to hlavne svetelné detektory, laserové aktívne záclony a pasívne a aktívne infračervené detektory so záclonovou charakteristikou.

1.4.2 Detektory priestorovej ochrany

Detektory pohybu priestorovej ochrany tvoria veľmi dobré doplnenie plášťovej ochrany, a tým zvyšujú bezpečnosť objektu. Ťažiskom priestorovej ochrany sú centrálne body budovy akými sú schody, prístupové haly, chodby a vnútorné komunikačné uzly. Výhodou detektorov priestorovej ochrany sú nižšie náklady na inštaláciu a montáž a jednoduchosť montáže.

Základné delenie detektorov pohybu:

- VKV detektory,
- mikrovlnné detektory,
- ultrazvukové detektory,
- pasívne infračervené detektory,
- aktívne infračervené detektory,
- duálne, kombinované detektory. [7]

1.4.2.1 VKV detektory

VKV detektory sú najstaršie priestorové detektory, ktoré pracujú v oblasti veľmi krátkych vĺn na frekvencii zhruba 420 MHz.

Pracujú buď ako delené VKV detektory, ktoré majú oddelenú samostatnú vysielaciu a prijímaciu časť. Pracujúce na princípe zmeny homogenity elektromagnetického poľa vytvoreného v chránenom objekte, v priestoroch medzi vysielacou a prijímacou anténou. Táto zmena homogenity elektromagnetického poľa, ktorú chápeme ako narušenie chráneného priestoru, spôsobí odraz elektromagnetického poľa vyžiareného vysielacou anténou. Na prijímacej strane detektoru nastane fázový posun signálu, ktorý je vyhodnocovaný a pri prekročení nastavenej medznej hodnoty detektor vyhlási poplach.

VKV detektory tiež môžu pracovať monolitne, to znamená, že vysielacia, vyhodnocovacia a prijímacia časť sú v jednej rovine a detektor pracuje na princípe Dopplerovho efektu. Princíp spočíva v tom, že vysielač vysiela elektromagnetické vlny danej frekvencie, prijímač prijíma odrazené elektromagnetické vlnenie a kmitočet vyhodnocuje elektronická časť. Ak sa vyslané elektromagnetické vlnenie odráža od statických, nepohyblivých objektov, interferencia je nulová, Ak sa objekt pohybuje, dochádza ku zmene kmitočtu odrazeného elektromagnetického vlnenia a je indikovaná zmena interferenčnej frekvencie.

1.4.2.2 Mikrovlnné detektory

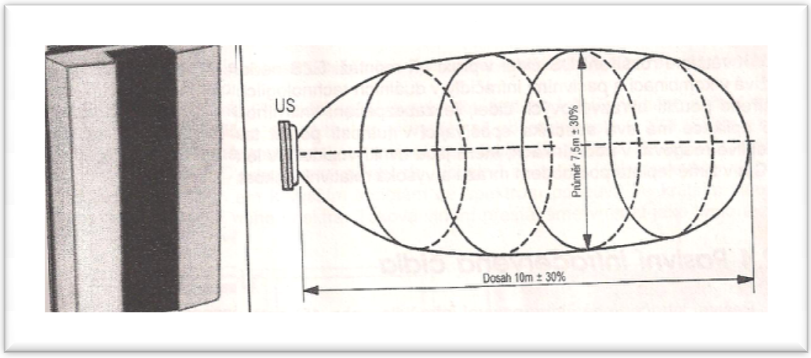
Mikrovlnné detektory, sú veľmi spoľahlivé a použiteľné u vysokých rizikách bezpečnosti, pretože zaisťujú najvyšší možný stupeň priestorovej ochrany a pri správnej inštalácií sú takmer neprekonateľné. Fungujú na princípe dopplerovho javu rovnako ako u VKV detektoroch, ale pracujú v kmitočtovom pásme elektromagnetického vlnenia 2,5 GHz, 10 GHz alebo 24 GHz. Najväčšia citlivosť mikrovlnného detektoru je v ose žiariča a najmenšia v kolmom smere k ose žiariča. Tieto detektory sa nemôžu montovať v priestoroch, kde môže dôjsť k elektromagnetickému rušeniu, tiež v blízkostiach zrkadiel či ochranných fólií. Musíme myslieť aj na to, že je možnosť vzniku falošných poplachov z dôvodu, že mikrovlny čiastočne prenikajú sklenenými plochami a tenkými stenami. [7]

1.4.2.3 Ultrazvukové detektory

Aktívne detektory, vyžarujúce ultrazvukové pole na frekvencii v pásme 20 – 45 KHz, pracujú na princípe Dopplerovho javu. Aktívnym prvkom je akustický žiarič (vysielač), ktorý vysiela do chráneného priestoru vlnenie o stálom kmitočte nad počuteľným pásmom zvuku, ktorý niektoré zvieratá počujú. Ak sa zmení prijatá vlna od vyslanej, zmena fáze, vyhodnotí sa to ako poplach.

Zásady montáže ultrazvukových detektorov:

- miesto inštalácie detektoru má byť navrhnuté tak, aby sa potenciálny páchateľ pohyboval smerom k detektoru alebo od detektora,
- dosah detektoru väčšinou nepresahuje vzdialenosť 10 m,
- čím tvrdší a hladší povrch telies v dosahu detektoru, tým je intenzívnejší odraz,
- Dopplerov efekt môže byť ovplyvnený prúdením vzduchu, preto by ultrazvukové detektory nemali byť inštalované v prievane alebo v blízkosti kúrenia, či ventilácie,
- ultrazvukové vlny neprenikajú stenami ani sklom.



Obrázok 9 Ultrazvukový detektor a jeho charakteristika [7]

1.4.2.4 Pasívne infračervené detektory

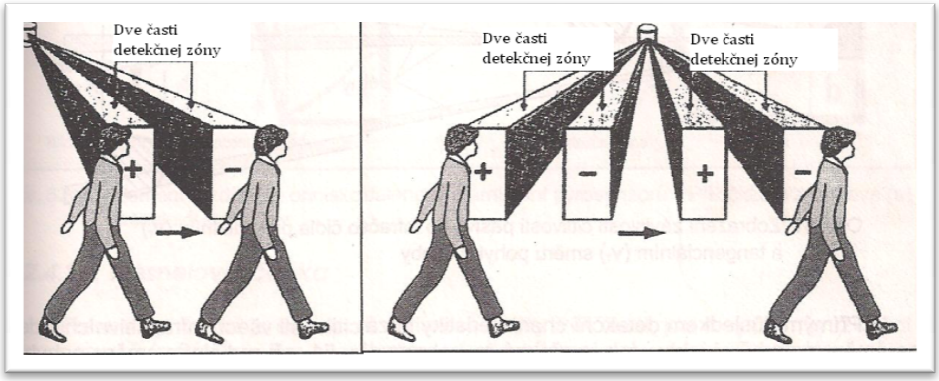
Ide o v dnešnej dobe najrozšírenejší druh priestorovej ochrany, označovaný ako PIR detektor. Vyznačujú sa veľkou spoľahlivosťou, ľahkou montážou a nízkou spotrebou energie. Do jednej miestnosti je možné inštalovať viacej detektorov tohto druhu, pretože nevyžarujú žiadnu energiu. PIR detektory slušne bojujú proti vznikom falošných poplachov, no aj tak existuje veľa faktorov, ktoré ovplyvňujú ich činnosť.

- svetelné rušenie (slnko, svetlomety automobilov...),

- rýchle teplotné zmeny (podlahové kúrenie, krb...),
- faxovacie prístroje,
- zvieratá,
- prúdenie vzduchu.

Princíp činnosti PIR detektorov spočíva v detekcii spektra infračerveného žiarenia, ktoré vyžaruje narušiteľ. Každý pasívny infračervený detektor obsahuje pyroelement, čo je polovodičová súčiastka s najvyššou citlivosťou posunutou do oblasti infračerveného žiarenia. Pyroelement je menič gradientnej povahy, čo znamená, že detekuje zmeny dopadajúceho žiarenia. Ak sa pohybuje v stráženom priestore osoba s teplotou inou ako teplota prostredia, zachycuje detektor odchýlky od normálneho stavu teploty okolia v závislosti na čase. Tie sú elektronikou zasielané a vyhodnocované ako poplach.

Klasický pyroelement reaguje aj na nepohyblivý zdroj žiarenia, ktorý dostatočne rýchlo mení svoju teplotu, a tým vznikajú falošné poplachy. Kvalitné PIR detektory obsahujú dva pyroelementy, zapojené v sérií ale opačne polarizované . Ich výstupné signály sa sčítajú a tým sa detekuje iba pohyblivý zdroj žiarenia, ak súčet pyroelementov bude odlišný od nuly. [7]



Obrázok 10 Detekcia Dual a Quadro [7]

1.4.2.5 Aktívne infračervené detektory

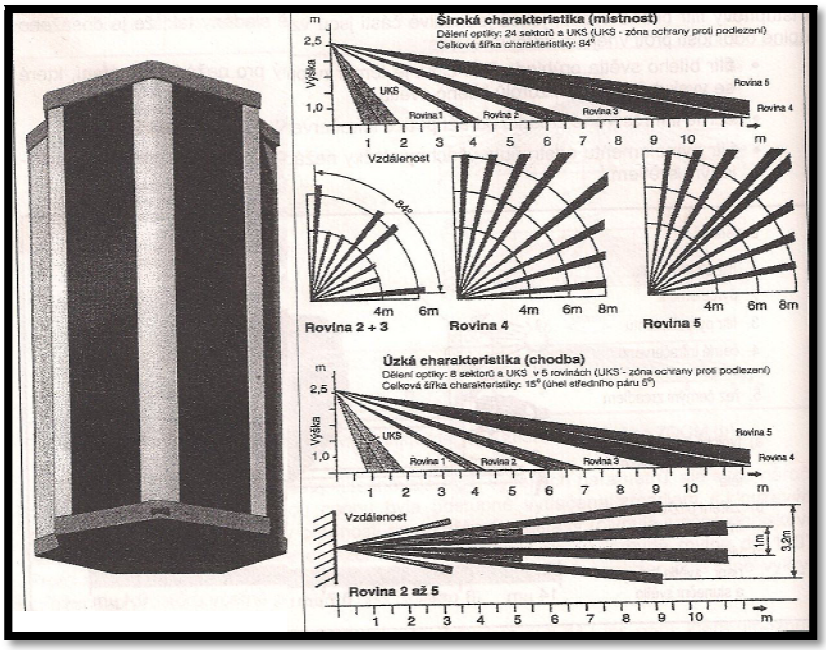
Ide o nový princíp aktívneho detektoru pohybu, ktoré sa označuje AIR (Activ Infra Red). Je vhodný pre stráženie v priestoroch vyžadujúcich vysoký stupeň zabezpečenia.

Princípom činnosti je vysielanie kódovaných lúčov v blízkom infračervenom pásme a príjem odrazu, digitalizácia a vyhodnocovanie signálu. Šošovková optika zaistí rozdelenie infračerveného žiarenia do jednotlivých aktívnych sektorov. Tento detektor je schopný detekcie v stráženom priestore pohyb telesa, ktoré nevyžaruje teplo a aj teleso pohybujúce sa veľmi nízkou rýchlosťou. Aktívny infračervený detektor pracuje na princípe porovnávania do pamäti uložené reflexné štruktúry stráženého priestoru, so štruktúrou v dobe uvedenia detektoru do stavu stráženia. Využíva vlnové dĺžky vzdialené od stredu typického vyžarovania živým objektom. Veľkou výhodou je možnosť zmeny detekčnej charakteristiky preprogramovaním a to na 84° alebo 14°. Jeho dosah je až 12m. Na rozdiel od PIR detektora nemá odraz svetla reflektorov ani slnečného žiarenia vplyv na vznik planých poplachov.

Možnosti aplikácií aktívneho infračerveného detektora:

- v miestnostiach s klimatizáciou,
- v miestnostiach s možnosťou rýchlych zmien teplôt,
- v miestnostiach s podlahovým kúrením,
- k zabezpečeniu predmetov uložených vo vitrínach, za sklom,
- pri veľmi malom pohybovaní sa narušiteľa, pričom nezáleží na smere pohybu.

Tento detektor je možné umiestniť vo vnútri budovy na sledovanie vonkajšieho priestoru, alebo s použitím vhodných krytov je možnosť tento detektor využiť ako vonkajšiu ochranu a tiež sa využíva na predmetovú ochranu. Nevýhodou tohto detektoru je veľmi vysoký odber prúdu oproti iným priestorovým detektorom, mŕtvy čas po zapnutí detektoru, ktorý trvá približne 3 sekundy, kedy sa detektor informuje o stráženom priestore. Ďalšou nevýhodou je vyžarovanie infračerveného žiarenia, ktoré je možné ľahko identifikovať a zistiť tým mŕtve zóny a aktivitu detektora. [7]



Obrázok 11 AIR a jeho priestorová charakteristika [7]

1.4.2.6 Kombinované duálne detektory

Kombinácia dvoch detektorov pracujúcich na rôznych fyzikálnych princípoch je veľmi spoľahlivé riešenie detekcie s minimálnym, zanedbateľným rizikom vzniku falošného poplachu. Ide o dva rôzne fungujúce detektory v jednom obale. Väčšinou sa spojujú pasívne infračervené detektory s mikrovlnnými detektormi, menej často s detektormi pracujúcimi s ultrazvukovými vlnami. Výstupnú informáciu kombinovaných detektorov spracováva logika, ktorá vyhlási poplach iba ak súčasne alebo v krátkom časovom intervale dôjde k detekcii v oboch častiach duálneho detektora. Je možné detekovať narušiteľa v každom systéme zvlášť. V prípade poruchy jedného systému je možnosť nastavenia duálneho detektoru tak aby sa narušiteľ detekoval iba pomocou jedného funkčného systému. Duálne detektory sú veľmi spoľahlivou ochranou v priestoroch s vysokým stupňom zabezpečenia. [7]

1.4.3 Detektory predmetovej ochrany

Prvky predmetovej ochrany sú predovšetkým určené k ochrane cenných predmetov, akými sú obrazy, skrine, sochy, trezory. V našom prípade môžu slúžiť hlavne na ochranu utajovaných informácií, či informácií know – how.

Na ochranu predmetov sa využívajú tieto detektory:

- kontaktné detektory,
- kapacitné detektory,
- tlakové akustické detektory,
- bariérové detektory,
- trezorové detektory,
- detektory na ochranu umeleckých predmetov.

1.4.3.1 Kontaktné detektory

Zaraďujeme sem:

- tlakové kontakty – inštalujú sa tam, kde je riziko zdvihnutia predmetu,
- ťahové kontakty – obsahuje dva kontakty a ťažné lano alebo kábel, ktorý reaguje na zmenu vopred nastaveného napätia v ťahu, (ochrana technologických prechodov, šachiet),
- mikrospínače,
- magnetické kontakty.

1.4.3.2 Kapacitné detektory

Najstarší používaný druh aktívnych elektronických detektorov. Jeho hlavným cieľom je indikovať priblíženie sa alebo dotknutie nepovolanej osoby stráženého predmetu. Tieto detektory sú určené k stráženiu obrazov, voľne stojacich predmetov, ale aj skríň a rôznych priechodov. Kapacitný detektor je konštruovaný ako doskový kondenzátor, ktorého jedna elektróda je kovová časť predmetu a druhá elektróda je zem. Využíva elektrických vlastností kondenzátoru, medzi elektródami je vytvorené elektrostatické pole. Ak vložíme do elektrostatického poľa nejaký predmet, zmení sa kapacita kondenzátora. Ak zmena presiahne vopred nastavenú hodnotu, procesor vyhlási poplach. Jeho najväčšou prednosťou je, že k vyhláseniu poplachu môže dôjsť už v čase prítomnosti páchateľa, skôr než sa vôbec predmetu dotkne. [7]

1.4.3.3 Tlakové akustické detektory

U predmetovej ochrany sa využívajú na zaistenie exponátov v dobre utesnených vitrínach. Je vhodné ich použiť aj na predmety s vysokým stupňom zabezpečenia.

1.4.3.4 Bariérové detektory

Sú to detektory reagujúce na narušenie bariéry, ktorá je vytváraná vyžarovacou alebo snímacou charakteristikou. Patria sem:

- laserové detektory s charakteristikou záclony,
- infračervené závory, záclony a bariéry,
- pasívne infračervené detektory s charakteristikou záclony,
- aktívne infračervené detektory s charakteristikou záclony.

1.4.3.5 Trezorové detektory

K ochrane trezorov a trezorových miestností sa používajú trezorové seizmické detektory, ktoré sú schopné rozpoznať všetky, dnes známe spôsoby napadnutia spomínaných priestorov. Používa široký frekvenčný rozsah a tri nezávisle pracujúce vyhodnocovacie kanále, na detekciu použitia rôznych výbušnín, mechanického a tepelného náradia či špeciálneho elektrického rotačného náradia. Tieto trezorové detektory pracujú na princípe selektívneho vyhodnotenia vlnenia. Vlnenie sa šíri ako zvuková vlna, ktorá je zachytávaná piezoelektrickými keramickými snímačmi napevno namontovanými na trezor. Elektronické zariadenie je vybavené vyhodnocovacím obvodom schopným detekovať všetky signály spôsobené mechanickými, termickými nástrojmi, alebo signály špecifického priebehu akými sú napríklad výbušniny. U týchto typov detektorov je veľká pozornosť tiež venovaná ochrane proti sabotáži a to pomocou ochranných kontaktov a obvodov pre kontrolu teploty a cudzích magnetických polí. [7]

1.4.3.6 Detektory na ochranu umeleckých predmetov

Táto skupina detektorov je určená na ochranu umeleckých predmetov, akými sú obrazy, sochy, gobelíny, umiestnené v galériách či múzeách. Tieto detektory sú navrhnuté tak, aby

predmety trvale strážili bez prestávky a to aj v čase prevádzky. Na ochranu umeleckých predmetov sa používajú tieto detektory:

- závesové detektory – vyhodnotené sú veľmi malé pohyby stráženého predmetu zaveseného tenkým nerezovým drôtom na hák závesového detektora,
- polohové detektory – pomocou mechanického kontaktu sníma pohyb plátna obrazu,
- váhové detektory –umiestňuje sa pod strážený predmet (soška, váza), vyhodnocuje zmenu hmotnosti, ktorú detektor porovnáva s hmotnosťou zaznamenanou po pripojení detektoru k napájaciemu napätiu,
- optické detektory. [7]

1.4.4 Detektory obvodovej ochrany

Zaistenie perimetrickej ochrany je veľmi dôležitá a náročná činnosť, pri ktorej je nutné použiť detektory schopné fungovať aj vo veľmi nepriaznivých vonkajších prevádzkových podmienkach. Je nutné kombinovať a integrovať oveľa viac postupov a prvkov ako u ochrany vnútorných priestorov, či predmetov. Na trhu je obrovské množstvo detektorov perimetrickej ochrany, pracujúcich na rôznych fyzikálnych princípoch, zamerané na rôzne druhy ochrany majetku. Dôležité je, aby konštrukcia detektorov bola prispôsobená vonkajším vplyvom. Musí mať odlišné napájanie ako u bežných detektorov a v neposlednom rade musíme myslieť na fakt, že detektory určené na obvodovú ochranu musia mať niekoľkonásobné väčší dosah ako bežné detektory. Ďalším dôležitým faktom je, že detektory nesmú byť citlivé na širokú škálu činností, ktoré sa nachádzajú v bežnej prírode napríklad vlnenie trávy či pohyb lístia.

Detektory na obvodovú ochranu sa prvotne delia na:

- pasívne,
- aktívne.

Pasívne detektory obvodovej ochrany pasívne registrujú fyzikálne zmeny vo svojom okolí. Sú ťažšie identifikovateľné, pretože do priestoru nevyžarujú žiadnu energiu.

Sú to:

- plotové vibračné detektory,
- plotové tenzometrické detektory,
- mikrofóne káble,

- systémy strážiace drôtovú osnovu,
- diferenciálne tlakové detektory,
- detektory magnetických anomálií,
- seizmické detektory,
- vláknovo optické systémy,
- perimetrické pasívne infračervené detektory,
- infračervené termovízne detektory.

Aktívne detektory obvodovej ochrany aktívne zasahujú do okolitého priestoru. Nevýhodou je ich ľahká detekcia a zistenie mŕtvych zón.

Sú to:

- štrbinové káble,
- infračervené bariéry a závory,
- laserové závory,
- laserové rádiolokátory,
- aktívne infračervené detektory,
- mikrovlnné detektory,
- dvojité mikrovlnné detektory,
- kombinované, duálne detektory,
- kombinované, mikrovlnné – infračervené detektory,
- reflexné detektory dynamických zmien elektrického poľa,
- kapacitné detektory. [7]

1.4.4.1 Plotové vibračné detektory

Tieto detektory sú určené na ochranu oplotených objektov, ktorých plot je vyrobený z drôtu, mreží, či ostnatého drôtu. Systém využíva odrazov elektromagnetickej vlny na vedení, ktoré tvorí dvojdrôtová linka s vibračnými snímačmi. Elektronické zariadenie generuje impulzné signály pre detekčné vedenie a zároveň vyhodnocuje signály odrazené z tohto vedenia. Stav detekčného vedenia je vyhodnocovaný podľa charakteru odrazených impulzov. Na to, aby sa vyhlásil poplachový stav musia nastať minimálne 3 poplachové podnety v určitom rozsahu vzdialeností a v určitom časovom intervale.

Plot je nutné deliť na úseky s dĺžkou 150 m. Pre elimináciu vplyvov, ktoré pôsobia na veľkej dĺžke perimetru systém používa detekčnú meteorologickú jednotku, ktorá sníma a vyhodnocuje rýchlosť vetra a efektívne kompenzuje tieto vplyvy. Tento druh detekcie sa vyznačuje ľahkou montážou, prijateľnou cenou ale má jednu veľkú nevýhodu a to ľahkú možnosť prekonania a možnosť obmedzenia reakčnej zóny mechanickou fixáciou v blízkosti miesta prieniku.

1.4.4.2 Plotové tenzometrické detektory

Tenzometrické detektory využívajú kombináciu mechanickej a elektronickej ochrany. Mechanickú ochranu tvoria špeciálne žiletkové, ostnaté alebo hladké drôty vo dvojiciach s rozstupom približne 10 cm. Systém je nastavený tak, aby pri záťaži väčšej ako 15 kg došlo k vyvolaniu poplachu. Drôtová osnova je vytváraná po 45 metrových úsekoch. Uprostred každého úseku je senzorový stĺp. Elektronická ochrana spočíva vo vyhodnocovaní ťahovej diferencie drôtu. Veľkou nevýhodou tohto systému sú vysoké investičné náklady.

1.4.4.3 Systémy strážiace drôtovú osnovu

Tento systém je určený ku stráženiu stavu oplotenia prúdovými slučkami v signálnej osnove. Princípom je vyhodnocovanie nízkonapäťových impulzov, ktoré sa šíria v signálnej osnove, ktoré sú vyhodnocované po priechode slučkami osnovy úsekovým zariadením. Meria a porovnáva ich amplitúdy a kmitočet. Je dôležité vodiče montovať skryto, kvôli možnosti prekonaniu páchateľom. [7]

1.4.4.4 Mikrofóne káble

Primárny detekčný systém obvodovej ochrany pre objekty stredného až vysokého rizika, alebo záložný a doplnkový systém pre obvodovú ochranu objektov s vysokým stupňom rizík. Takto by sme mohli určiť použitie mikrofónných káblov, ktoré umožňujú chrániť pletivové a zvárané ploty a oplotenia z betónových dielcov. Tento spôsob detekcie umožňuje indikovať pokusy o prienik chránenou plochou, demontáž, rezanie, úmyselné poškodenie aj pokus o neoprávnenú manipuláciu. K detekcii sa používajú dva typy káblov:

- mikrofóne káble s diskrétnymi snímacími prvkami,
- mikrofóne koaxiálne káble s rozloženými snímacími parametrami.

1.4.4.5 Diferenciálne tlakové detektory

Ide o hydraulické podzemné detektory, ktoré pre detekciu narušenia využívajú kompenzačnú metódu. Princíp spočíva v paralelnom uložení dvoch pružných detekčných hadíc s roztečou 1-1,5 m, po celom obvode chráneného pozemku. Hadice je potrebné uložiť 25 – 30 cm pod povrch zeme do pieskovej lóže. Vďaka paralelnému uloženiu hadíc sa vylučujú falošné poplachy spôsobené vzdialenými podnetmi akými je napríklad frekventovaná cesta. Hadice sú natlakované tlakom 250 – 300 kPa ekologickou nemrznúcou kvapalinou. K citlivým senzorom sú prenášané tlakové prejavy vznikajúce na povrchu zeme. Poplach je signalizovaný po elektronickom vyhodnotení týchto prejavov ako prekročenie prahovej hodnoty. Veľkou výhodou diferenciálnych tlakových detektorov je možnosť pôdorysného kopírovania akéhokoľvek terénu po obvode pozemku.

1.4.4.6 Seizmické detektory

Tieto detektory sa používajú k perimetrickej ochrane vo voľnom teréne. Senzor je veľmi citlivý mikrofón (elektrétový mikrofón), upevnený vo vodotesnom držiaku, inštalovanom v pieskovej lóži pod zemou asi 50 cm. Jednotlivé senzory sa umiestňujú vo vzdialenosti 50 – 100 m od seba. Princíp spočíva vo vyhodnotení prekročenia limitnej hodnoty otrasu, ktorý zaznamenajú citlivé senzory. Tento typ detekcie sa používa v ojedinelých prípadoch aj k operatívnemu nasadeniu vo voľnom teréne. V takomto prípade sa snímače umiestňujú iba pár centimetrov pod povrch zeme, čo umožňuje detekciu krokov v dosahu až 50 m od detektora. [7]

1.4.4.7 Detektory magnetických anomálií

Sú to citlivé senzory vo forme dosky, tyče alebo snímacích káblov, ktoré sú uložené v zemi pod ľubovoľným terénom vrátane asfaltu, betónu a dokonca aj pod vodnou hladinou. Princíp detektoru spočíva vo vyhodnocovaní anomálií v magnetickom poli Zeme. Vyhodnocujú sa zmeny magnetického toku v slučke senzoru, ktoré nastávajú pri pohybe

narušiteľa, feromagnetického materiálu v okolí senzora. Slučky sú tvorené závitmi pancierovaného káblu a vždy musia mať párny počet. Maximálna dĺžka slučky je až 500m. Zmeny magnetického toku spôsobujú vznik malých prúdov v slučkách, ktoré sú ďalej spracovávané. K vyhláseniu narušenia musia byť v jednom úseku, v danom časovom okne a intervale, zaznamenané dva poplachy od dvoch slučiek. Veľkou výhodou je nielen rôznorodosť povrchu, pod ktorým môže byť detektor použitý, ale aj to, že tento druh detekcie umožňuje určiť aj smer pohybu narušiteľa. Ďalším plusom je odolnosť falošných poplachov, ktoré spôsobujú vtáky, iná zver, poveternostné podmienky a rušivých geomagnetických vplyvov akými sú búrky a rádiové vysielače.

Detektory magnetických anomálií je veľmi spoľahlivý spôsob ochrany, ktorý sa používa vo veľkých strážených priestoroch akými sú letiská, či armádne základne.

1.4.4.8 Vláknové optické systémy

Detekciu zaisťuje telekomunikačné optické vlákno, svetlovod, pre infračervenú oblasť.

V obvodovej ochrane sa používajú:

- svetlovodné senzorové káble,
- opticko – mechanické systémy,
- svetlovodné zábranné siete.

Vhodným uložením svetlovodu je možné určiť, či sa jedná o stojaci alebo pohybujúci sa objekt a miesto napadnutia. Pri použití dvojici vlákien systém dokáže určiť aj smer a rýchlosť pohybu narušiteľa a aj to, či ide o človeka alebo zviera. Dĺžka slučky môže byť až 40 Km. [7]

1.4.4.9 Perimetrické pasívne infračervené detektory

Nazývame ich infrateleskopy a fungujú na rovnakom princípe ako PIR pre vnútorné použitie. Dve zbiehavé detekčné zóny tvaru záclony s prienikom v mieste detektora, zachytávajú tepelné žiarenie, ktoré vyžaruje narušiteľ. Toto žiarenie pri pohybe narušiteľa mení snímaný tepelný obraz. Aj malá zmena teploty v detekčnej zóne vyvolá poplach. Dosah infrateleskopu je 50 – 150 m. Použitím viacnásobných pyrosenzorov (Quadro), je

vznik falošných poplachov spôsobovaných vírením vzduchu, slnkom, či reflektormi áut, eliminovaný na minimum.

1.4.4.10 Infračervené termovízne detektory

Tieto detektory využívajú princíp termovíznej kamery. Tá sníma tepelné žiarenie emitované objektmi pozorovanej scény a tepelné žiarenie, ktoré sa od nich odráža. Na televíznej obrazovke je elektronicky spracovaný a zobrazený tepelný obraz vznikajúci na základe odlišných tepelných profilov objektov od pozadia. Termovízna kamera je veľmi účinné zariadenie, ktoré je schopné plnohodnotne pracovať za všetkých svetelných podmienok, v noci, aj v snežení. Na stráženie perimetra sa používa v stacionárnom prevedení s motorickým kĺbovým držiakom a s diaľkovým ovládaním. Jej dosah je približne 1500 m.

1.4.4.11 Štrbinové káble

Ďalší spôsob obvodovej ochrany, ktorý vytvára neviditeľnú bariéru. Systém pracuje na princípe radarovej detekcie. Pohyb je detekovaný pomocou elektromagnetického poľa medzi dvoma štrbinovými káblami, ktoré sú uložené paralelne pod alebo nad povrchom zeme.

Typy prevedenia:

- dva štrbinové káble,
- dvojitý integrovaný štrbinový kábel,
- mobilná verzia štrbinových káblov. [7]

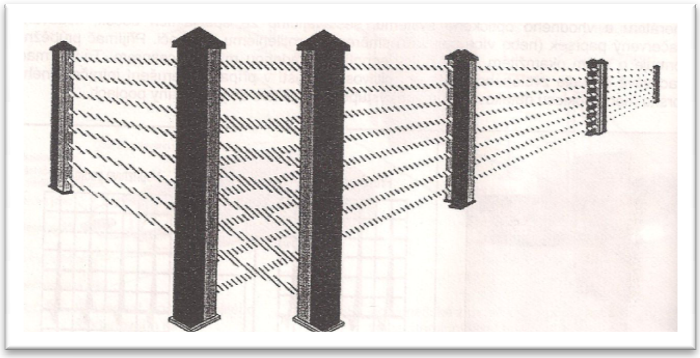
1.4.4.12 Infračervené závory a bariéry

Tento druh detekcie je jeden z najrozšírenejších v oblasti obvodovej ochrany. Jeho cieľom je signalizácia vniknutia nepovolanej osoby za obvod strážených objektov.

Infračervené závory pracujú vždy v páre. Obsahujú vysielač na jednej strane a prijímač na strane druhej. Vysielač vysiela pomocou generátora a optického systému kódovaný infračervený lúč smerom k protiľahlému prijímaču. Pri prerušení prijímaného

infračerveného lúča prijímač vyšle informáciu riadiacej jednotke a tá vyvolá poplach. K obmedzeniu vzniku falošných poplachov vyvolaných vtákmi, alebo inou zverou, je vysielač nastavený tak, aby vysielal dva alebo viac synchronizovaných infračervených lúčov. Poplach je vyhlásený iba ak sú tieto lúče prerušené súčasne.

Infračervené bariéry sa skladajú zo stĺpika s rôznym počtom vysielačov a stĺpika s rovnakým počtom prijímačov. Každý pár stĺpikov je možné osadiť dvoma až desiatimi protiľahlými dvojicami, to zabezpečí systém paralelných IR lúčov. K zabráneniu vzájomných interferencií môže byť každá dvojica stĺpikov nastavená na jednu z viacerých možností modulačných frekvencií. Bezpečný dosah infračervených bariér je zhruba 150 m, niektorí výrobcovia udávajú aj viac.



Obrázok 12 Usporiadanie infračervených bariér [7]

Obrázok 13 Infračervená závora [20]

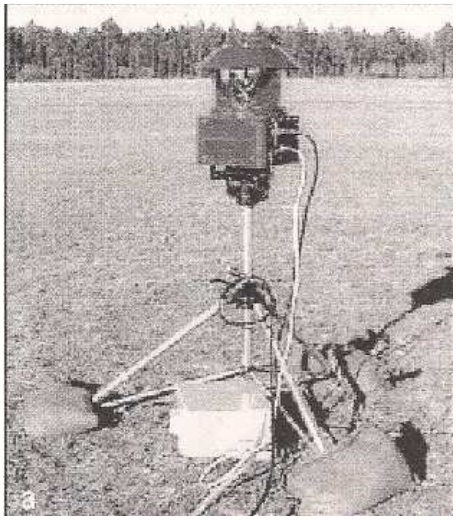
1.4.4.13 Laserové závory

Môžeme povedať, že ide o moderný systém ochrany perimetrie. Systém je zhodný s už spomínanými infračervenými závorami, ale namiesto infračerveného lúča vysielač vysiela zväzok laserových lúčov. Hovoríme o vlnovej dĺžke 850 nm vychádzajúceho z vysielača. Ohrozenie zraku laserový žiarením je v tomto prípade vylúčené. Rôzne zdroje falošných poplachov akými sú vtáci, padajúce predmety, iné zdroje svetla, sú systémom eliminované a nie sú vyhodnotené ako poplach. Táto eliminácia sa vykonáva na základe vyhodnotenia doby prerušenia efektívneho rovnobežného zväzku. Dosah tejto závory je až 1 km. Tento druh detekcia sa používa na zaistenie dlhých pozemkov, ciest a koridorov. [7]

1.4.4.14 Laserové lokátory

Názov je odvodený od anglických slov Light Detection And Ranger, Lidar. Používa sa pre detekciu pohybu narušiteľa v stráženom priestore pomocou modernej laserovej technológie. Využíva vlnovú dĺžku 905 nm. Tento systém detekcie je možné použiť pre stacionárne aj mobilné aplikácie a tiež ako predsunutý detekčný prostriedok, ktorý dokáže strážiť rozsiahlu plochu a obsahuje funkciu predpoplachu. Detekčná jednotka obsahuje mikropočítač, prostredníctvom ktorého sa vykonáva monitorovanie a ovládanie.

Zameriavače vysielajú laserové modulované lúče o priemere 30 mm, ktoré sa po odraze od okolitého predmetu časť rozptýli a časť z nich sa vráti späť. Po spracovaní odrazených lúčov sa vyhodnotí informácia o okamžitej vzdialenosti predmetu. V priebehu prvých ôsmych otáčok si systém vyhodnotí pozíciu predmetov a charakteristiku terénu. Lidar obsahuje obrazovku, ktorá slúži ako grafické užívateľské rozhranie na sledovanie stráženej oblasti a na základe informácií o pohybu narušiteľa je schopná vykresliť trasu jeho pohybu. Dosah detektoru Lidar je kruh o polomere 20 – 100 m. Vďaka vysokej pravdepodobnosti detekcie narušiteľa, vysokého rozlíšenia a flexibilného zaistenia je tento detektor využívaný pre objekty so stupňom zabezpečenia 3 a 4. Napríklad: jadrové elektrárne, väznice, letiská, objekty vysokej dôležitosti, strechy rozsiahlych budov, muničné sklady, štátne hranice, mobilné vojenské tábory a veľa iných. [7]



Obrázok 14 Mobilný laserový lokátor [7]

1.4.4.15 Mikrovlnné závory

Vytvárajú vysokofrekvenčné elektromagnetické pole medzi vysielačom a prijímačom. Prijímač detekuje a vyhodnocuje zmeny energie, ktoré vznikajú vstupom narušiteľa alebo iného predmetu do detekčného zväzku mikrovlnného žiarenia, ktorý má tvar rotačného elipsoidu. Zmeny veľkosti amplitúdy prijatého signálu sú priamoúmerné veľkosti a hustote predmetu, ktorý je detekovaný. Tým pádom je možné rozlíšiť veľkosť zachyteného predmetu. Mikrovlnné bariéry pracujú na kmitočte 2,5 – 24 GHz. Mikrovlnné závory s dlhým dosahom môžu strážiť až 450 m priestoru s priemerom detekčnej zóny do 12 m. Veľkou výhodou tohto typu detekcie je vysoká odolnosť voči poveternostným vplyvom. Využívajú sa na stráženie letísk a iných rozsiahlych priestorov.

1.4.4.16 Mikrovlnné radary

Mikrovlnné radary sú riešené ako monolitné, pracujúce na princípe Dopplerovho efektu. Princíp spočíva vo vysielaní vysielačom mikrovlnnej energie do objektu. Predmety nachádzajúce sa v objekte odrazia energiu späť k prijímaču ako bežný odraz od nehybného pozadia. Pokiaľ sa objekt pohybuje, je kmitočet odrazeného signálu posunutý vplyvom Dopplerovho efektu. Poplach sa vyhlási na základe zmeny prijímaného signálu. [7]

1.4.4.17 Prahové mikrovlnné detektory

Mikrovlnné detektory prahové bývajú vybavené elektronikou, ktorá je schopná obmedziť maximálny dosah detektoru. To umožní zamedziť falošné poplachy vzniknuté za požadovaným dosahom detekcie. Majú rôzne charakteristiky:

- mikrovlnné detektory prahové s prstencovou charakteristikou,
- mikrovlnné detektory prahové s dútnikovou charakteristikou,
- mikrovlnné detektory prahové so širokouhlou charakteristikou. [7]

1.4.4.18 Dvojité mikrovlnné detektory

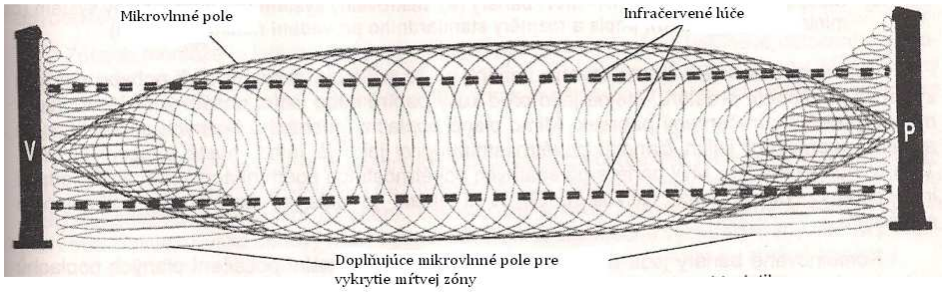
Detektor používa dva prijímacie kanály pracujúce s amplitúdovo modulovaným signálom, využívajúcich 5 nosných frekvencií v okolí pásma 10,5 GHz. Mechanizmus vylučuje slabé signály, signály odpovedajúce pohybu mimo rozsah nastavenej rýchlosti a signály, ktoré indikujú obojsmerný pohyb charakteristický pre porast a drobnú zver. Veľkosť detekčnej zóny je 25 x 25 m alebo 50 x 15 m pri dlhom dosahu. Obrovskou výhodou dvojitého detektoru je úžasná schopnosť vylúčiť zdroje falošných poplachov.

1.4.4.19 Duálne detektory

PIRAMID (PasiveInfra Red And Microwave Intruder Detector), je kombinovaný detektor určený pre priestorovú ochranu, využívajúci dvoch fyzikálnych princípov detekcie, aktívneho mikrovlnného a pasívneho infračerveného detektoru. Mikrovlnná jednotka vyhodnocuje pohyb na základe mikrovlnnej energie a pasívna infračervená jednotka detekuje tepelnú energiu pohybujúceho sa objektu. Na to, aby sa vyhlásil poplach musia narušiteľa detekovať obidva detektory súčasne. Detektor obsahuje dvojitú mikrovlnnú jednotku a dvojitý pyroelement. Duálny detektor týmto zamedzí vznik nežiaducich falošných poplachov. Použitie duálneho detektoru je rôznorodé, spravidla sa používa na ochranu plochých striech či vonkajších priestorov elektrární. Maximálny dosah je 35 m pri charakteristike s dlhým dosahom.

Kombinované mikrovlnné– infračervené bariéry sú bariéry pracujúce na princípe vysielania a prijímania infračervených lúčov spolu s mikrovlnnou formou detekcie. Obidva detektory sú inštalované spolu s vyhodnocovacou elektronikou na dvoch stĺpikoch, ktorých

vzájomná vzdialenosť môže byť až 150 m. Výška stĺpikov je iba okolo 150 cm. Takáto kombinovaná bariéra obsahuje mikrovlnný a infračervený systém a skrytú kameru, ktorá poskytuje majiteľovi okamžité overenie príčiny poplachu. Kombinované bariéry sú navrhnuté tak, aby minimalizovali vznik falošných poplachov na minimum, preto sú ideálnym riešením obvodovej ochrany v rozsiahlych priemyselných objektoch. [7]



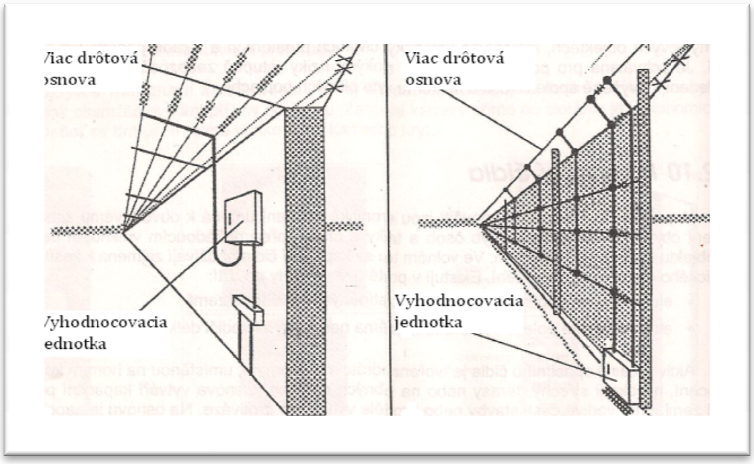
Obrázok 15 Detekčná charakteristika kombinovanej bariéry [7]

1.4.4.20 Kapacitné detektory

Reagujú na pohyb osôb a techniky a chránia pred vniknutím narušiteľa do objektu, alebo jeho opustením. Rozoznávame dva druhy použitia kapacitných detektorov:

- elektrostatické pole je vytvorené medzi netieneným vodičom a zemou,
- elektrostatické pole je vytvorené medzi dvoma netienenými vodičmi dĺžky až 150 m.

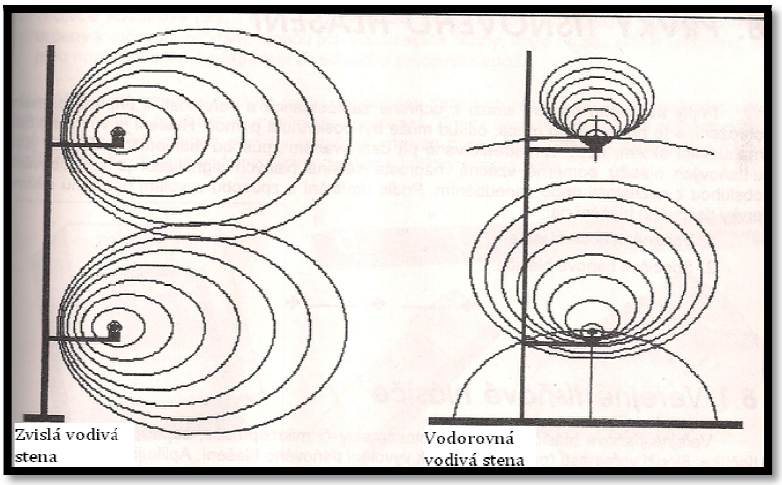
Aktívnu časť kapacitného detektora tvorí viacdrôtová osnova, ktorá je umiestnená na hornom konci plota alebo na okraji strechy. Táto osnova vytvára kapacitné pole proti zeme alebo vodivej časti stavby. Je na ňu napojený vstup jednotky, ktorý vyhodnocuje a spracováva zmenu kapacity. Detektor reaguje na prekročenie prahovej medze poplachu a aj na prerušenie drôtovej osnovy. Nevýhodou kapacitných detektorov je vysoký počet vzniku falošných poplachov, preto sa odporúča kombinovať tento detektor s ďalšími prvkami ochrany alebo druhom detekcie.



Obrázok 16 Kapacitný detektor na betónovom a drôtovom oplotení [7]

1.4.4.21 Reflexný detektor dynamických zmien elektrického poľa

Je to zariadenie, ktoré obsahuje vysielač sínusového signálu v pásme 18,182 kHz vyžarujúci do priestoru vlnu dlhú 16,5 km a prijímač so šírkou pásma 10 Hz, ktorý vyžiarenú vlnu prijíma. Vysielače vyžarujú intenzívne elektrické pole, ktoré je nežiarivé. Zmeny intenzity poľa, spôsobené nežiaducou osobou sú vyhodnocované obvodmi prijímača. [7]



Obrázok 17 Grafické zobrazenie elektrických polí vysielača a prijímača reflexného detektoru dynamických zmien [7]

2 TAKTICKO-TECHNICKÉ NÁVRHY NA ZEFEKTÍVNENIE OBJEKTOVEJ BEZPEČNOSTI

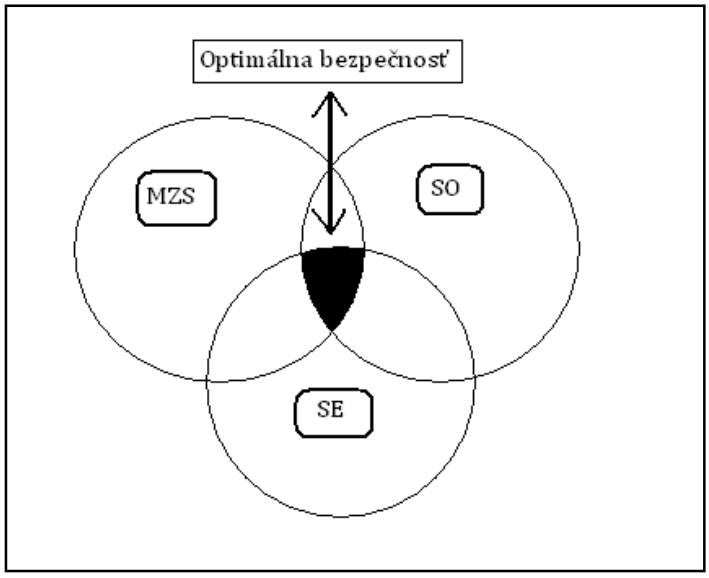
2.1 Integrované bezpečnostné systémy

Účinnú ochranu objektov je možné dosiahnuť iba ak vzájomne skombinujeme a usporiadame viac podsystémov bezpečnostných systémov a služieb. Vzájomnou koordináciou týchto bezpečnostných podsystémov sa vytvárajú Integrované bezpečnostné systémy. Integrovaný bezpečnostný systém slúži na zefektívnenie procesu ochrany a minimalizáciu hrozby chránených vzťahov. Všetko to je možné riešiť využitím technických prostriedkov na rýchlu elektronickú signalizáciu hrozby a mechanických zábran, ktoré vytvárajú účinný bezpečnostný systém. Štruktúru Integrovaného bezpečnostného systému tvoria poprepájané vzťahy medzi fyzickou ochranou, mechanickými zábrannými systémami, monitorovacími a signalizačnými zariadeniami a v neposlednej rade spolupráca so systémom organizačných opatrení. Jednotlivé prvky integrovaného bezpečnostného systému zaručujú vysokú flexibilitu a variabilitu, sú na sebe závislé, navzájom sa ovplyvňujú a pri nedostatočnej ochrane alebo zlyhaní jedného systému, je ohrozený celý komplex ochrany majetku. Tento systém znižuje riziko prekvapenia z útoku a tým vytvára priestor pre včasnú a primeraný reakciu. Kladne pôsobí na psychiku osôb, ktoré chráni. Cieľom integrácie služieb v komerčnej bezpečnosti je vytvoriť jeden funkčný celok technických prostriedkov v kombinácií s fyzickou bezpečnosťou a tým zvýšiť komfort ochrany majetku a bezpečnosť ochrany majetku. Na druhej strane integrácia systémov prináša bezpečnostnej službe zvýšenie pridanej hodnoty a konštantnú stabilitu ochrany majetku zákazníka.

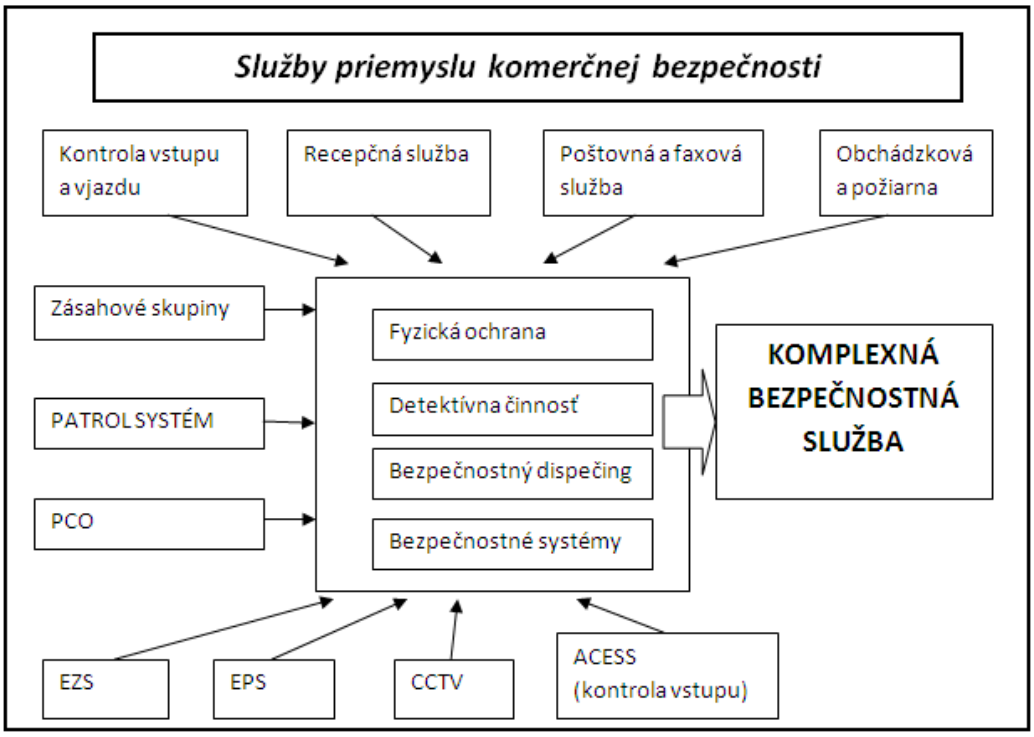
Mechanické zábranné systémy (MZS) sú systémy, ktoré tvoria komponenty mechanických a technických prostriedkov, komponentov a zariadení, ktoré sú skonštruované tak, aby znemožnili ich jednoduché prekonanie. Úlohou MZS je sťažiť alebo úplne znemožniť násilné vniknutie nepovolanej osoby do stráženého objektu a zabrániť neoprávnenej manipulácií s predmetmi nachádzajúcimi sa v stráženom objekte.

Monitorovacie a signalizačné systémy (SE) sú elektronické zariadenia, ktoré slúžia na včasnú registráciu a prenos informácií o napadnutí objektu, alebo o iných dôležitých informáciách o objekte.

Systém organizačných opatrení a fyzickej ochrany (SO) je systém, ktorého úlohou je prebratie informácie, o napadnutí objektu. Systém vyhodnotí vzniknutý aktuálny stav objektu, zabezpečí zákrok a prijatie zodpovedajúcich opatrení, na obnovu optimálneho stavu objektu. [10], [12]



Obrázok 18 Diagram optimálnej bezpečnosti [2]



Obrázok 19 Schéma služieb priemyslu komerčnej bezpečnosti a ich integrácia [10]

2.2 Integrované technologické systémy budov

Integrácia technologických systémov sa vykonáva u nových ale aj už existujúcich budovách. Integrované systémy v budovách zahŕňajú integráciu, správy a monitorovanie všetkých technologických a komunikačných systémov, podsystémov, či zariadení. Sú to systémy, ktoré zabezpečujú požadované funkčné parametre budov, kladú dôraz na integráciu vo forme otvoreného riadiaceho a komunikačného systému, ktorý umožňuje aktualizáciu a modifikáciu. Využívajú sa pri tom moderné prvky pre získavanie všetkých informácií o stave budovy v reálnom čase, spoľahlivé prostriedky pre prenos týchto informácií a riadiace systémy založené na distribuovaných počítačových systémoch. Integrovateľné komunikačné a riadiace systémy dokážu reagovať na nové požiadavky, ktoré vznikajú s novou dobou. Umožňujú aplikovať vyvíjajúce sa komunikačné a riadiace technológie bez väčších stavebných úprav a zásahov do objektu. [18]

2.3 Inteligentné budovy

Budovy, ktoré obsahujú integrované systémy sa väčšinou nazývajú inteligentné budovy. Inteligentné budovy sú objekty s integrovaným managementom, ktoré obsahujú zjednotené systémy riadenia technických systémov budov, bezpečnostnú technológiu a správu budov. Dokonalé a efektívne prostredie inteligentnej budovy je docielené optimalizáciou týchto zložiek a vzájomnou väzbou medzi nimi. Inteligentná budova vyjadruje poňatie prístupu k riešeniu.

Pre zabezpečenie skupinových požiadavkou musí byť vybudovaná externá sieť nadväzujúcich služieb, ktorých hlavným cieľom je zabezpečiť komplexné potreby obyvateľov inteligentného domu na základe určitých indikátorov monitorujúcich prostredie, stav systému a obyvateľov v budove.

Tabuľka 1 Triedy užívateľských požiadaviek na inteligentné budovy [18]

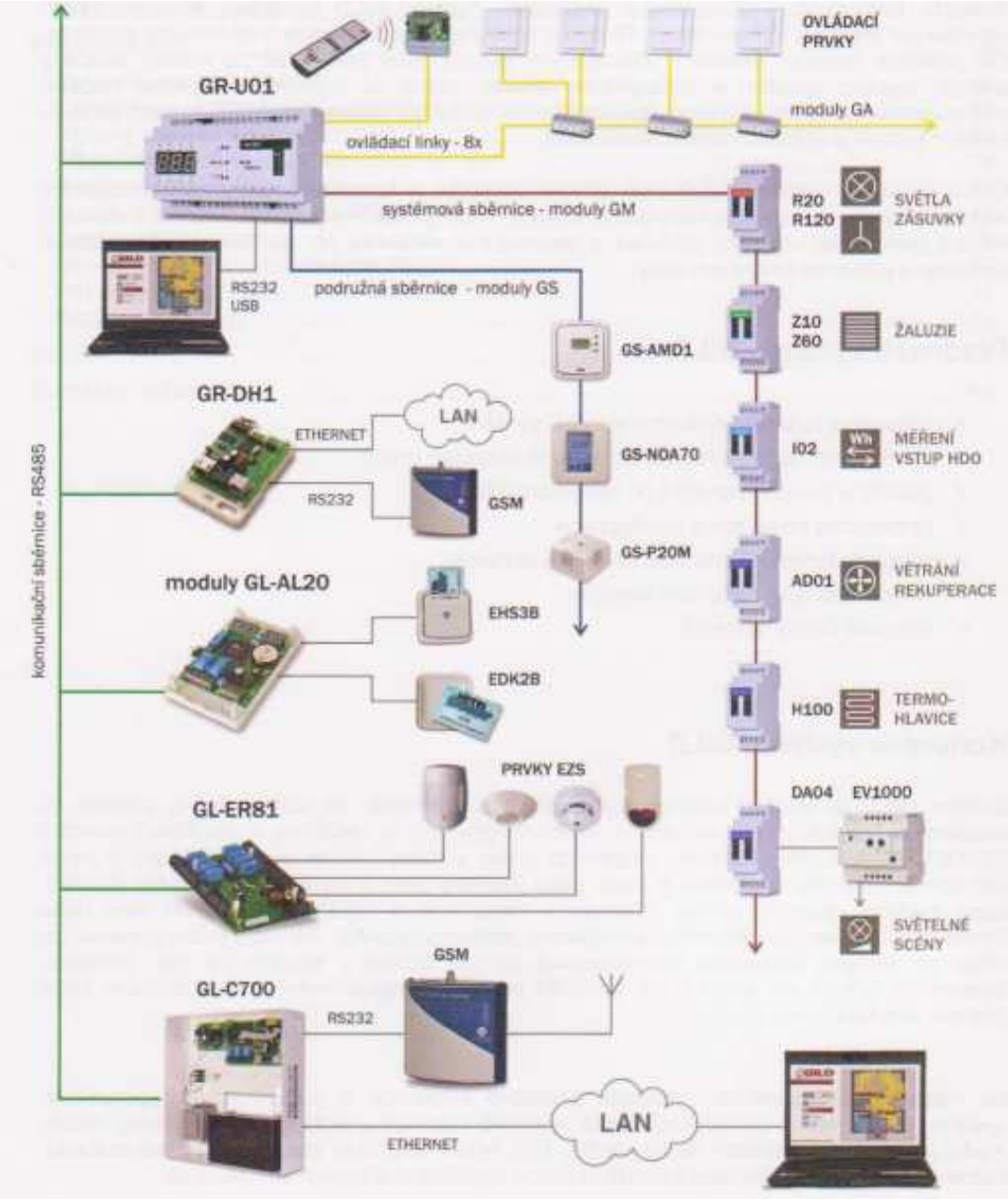
Technické požiadavky	**Užívateľské požiadavky**	**Sociálne požiadavky**
Spoľahlivosť a kvalita služieb	Užívateľské rozhranie	Bezpečnosť
Dostupnosť zariadení	Priateľské prostredie	Zdravotná a sociálna starostlivosť
Technika prostredia, spotreba energie a jej management	Nákladová bilancia	Kompatibilita s existujúcimi službami
Kompatibilita a zameniteľnosť	Možnosť personalizácie	Zabezpečenie súkromia
Komunikácia	Komfort a jednoduchosť užitia	Informačné služby

Inteligentné budovy vyžadujú:

- riadenie kvality vnútorného prostredia,
- energetický management, zahrňujúci technické alarmy,
- diaľkové meranie spotreby energií a médií,
- domový zabezpečovací a kamerový systém,
- domový informačný a riadiaci systém, ktorý zahrňuje simulácie prítomnosti, monitorovanie zdravotného stavu obyvateľov a ich bezpečnosti,
- detekciu neoprávneného vstupu,
- vzdialenú diagnózu systému, požiadavky na údržbu,
- vzdelávanie, e-learning,

- prácu z domu,
- videokonferenciu,
- spoločenskú starostlivosť,
- zábavu.

V budove, ktorú môžeme považovať ako inteligentnú budovu, zariadenia nekomunikujú iba v jednej triede systémov, ale je potrebné aby komunikovali medzi skupinami navzájom. Všetky požiadavky s každou skutočnosťou súvisia. Vykurovanie a chladiaci systém v budove sa riadi podľa prítomnosti ľudí, tiež osvetľovací systém v budove predstiera prítomnosť osôb a v čase ich neprítomnosti komunikuje s detektormi a zabezpečovacím systémom. Požiadavky na komunikáciu medzi skupinami a so službami si vyžadujú transparentný otvorený systém, ktorý sa jednoducho udržuje aktualizuje a voľne rozširuje. Toto všetko môže zaistiť iba otvorený zbernicový systém už spomínaných integrovaných systémov. [18]



Obrázok 20 Topológia zapojenia komponentov systému [19]

3 ZRANITEĽNOSŤ OBJEKTU A ANALÝZA ZRANITEĽNOSTI OBJEKTU

Základom analýzy zraniteľnosti objektu je odhalenie najslabšej časti skúmaného objektu. Je dôležité odhaliť kritické body a miesta v systéme ochrany objektu alebo chráneného záujmu. Analýza v sebe zahrňuje hodnotenie všetkých existujúcich skutočností, súvisiacich s bezpečnosťou chráneného záujmu. [3]

3.1 Bezpečnostná analýza

Analýzu môžeme charakterizovať ako expertnú bezpečnostnú činnosť, metódu poznania poznatkov a informácií o skúmanom bezpečnostnom objekte či situácií. Podstatou bezpečnostnej analýzy je rozdelenie celku na jednotlivé časti, následné štúdium a hodnotenie týchto častí a zistenie dôležitých informácií a vzájomných vzťahov medzi jednotlivými skupinami.

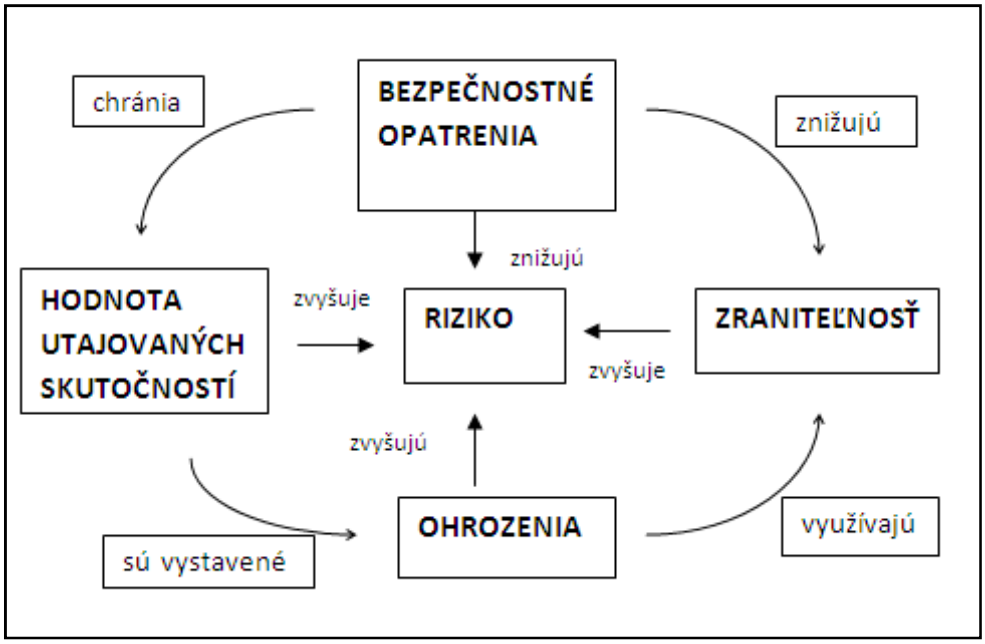
Prvým krokom k vykonaniu bezpečnostnej analýzy je stanovenie bezpečnostných rizík.

[1], [3]

3.1.1 Riziko

Riziko chápeme ako určitý druh neistoty, ktorý nám dokáže predpovedať vznik nepriaznivých skutočností. Je to akési možné nebezpečenstvo nepriaznivého vývoja.

„*V súvislosti s riešením fyzickej bezpečnosti a objektovej bezpečnosti budeme riziko chápať ako potenciálnu možnosť, že dané ohrozenie využije zraniteľnosť objektu (chráneného priestoru) na neoprávnenú manipuláciu s utajovanou skutočnosťou a môže tak spôsobiť ujmu Slovenskej republike.*“(Ing. Tomáš LOVEČEK, 2006)



Obrázok 21 Vzťahy ovplyvňujúce riziko [2]

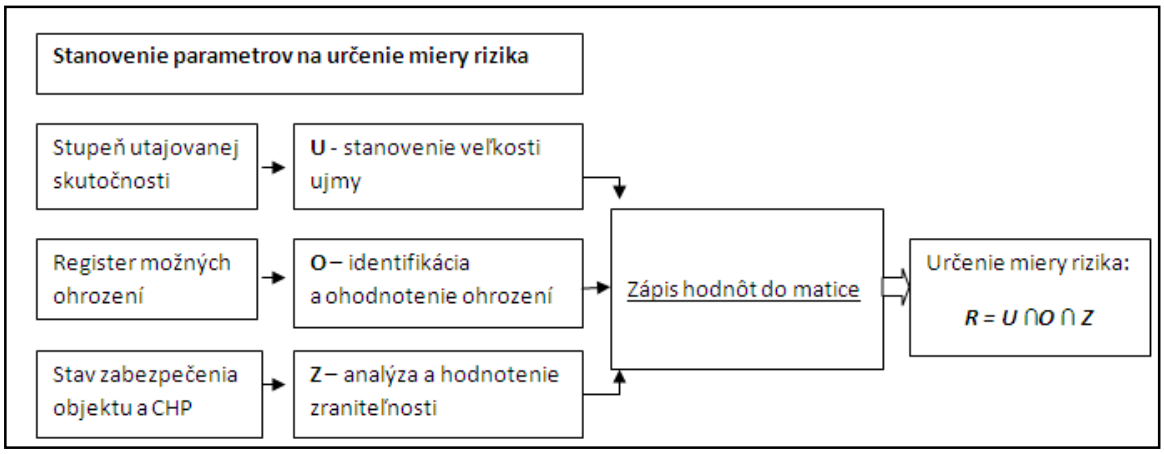
3.1.2 Analýza rizík

Analýza rizík je priebeh identifikovania rizík, hodnotenia ich veľkosti a zistenia ohrozenej oblasti, ktorú treba zabezpečiť bezpečnostnými opatreniami. Je to jedna z hlavných činností, ktoré je potrebné vykonať pred začatím projektovania každého bezpečnostného systému.

Cieľom analýzy rizík je

- určiť a oceniť riziká, ktoré ohrozujú alebo môžu ohroziť utajované skutočnosti,
- posúdiť nežiaduce dopady, ujmy, ktoré by mohli vzniknúť pri neoprávnenom zaobchádzaní s utajovanými skutočnosťami,
- určovať potrebné bezpečnostné opatrenia na zaistenie fyzickej a objektovej bezpečnosti. [2]

Na obrázku je znázornený základný algoritmus analýzy rizík.

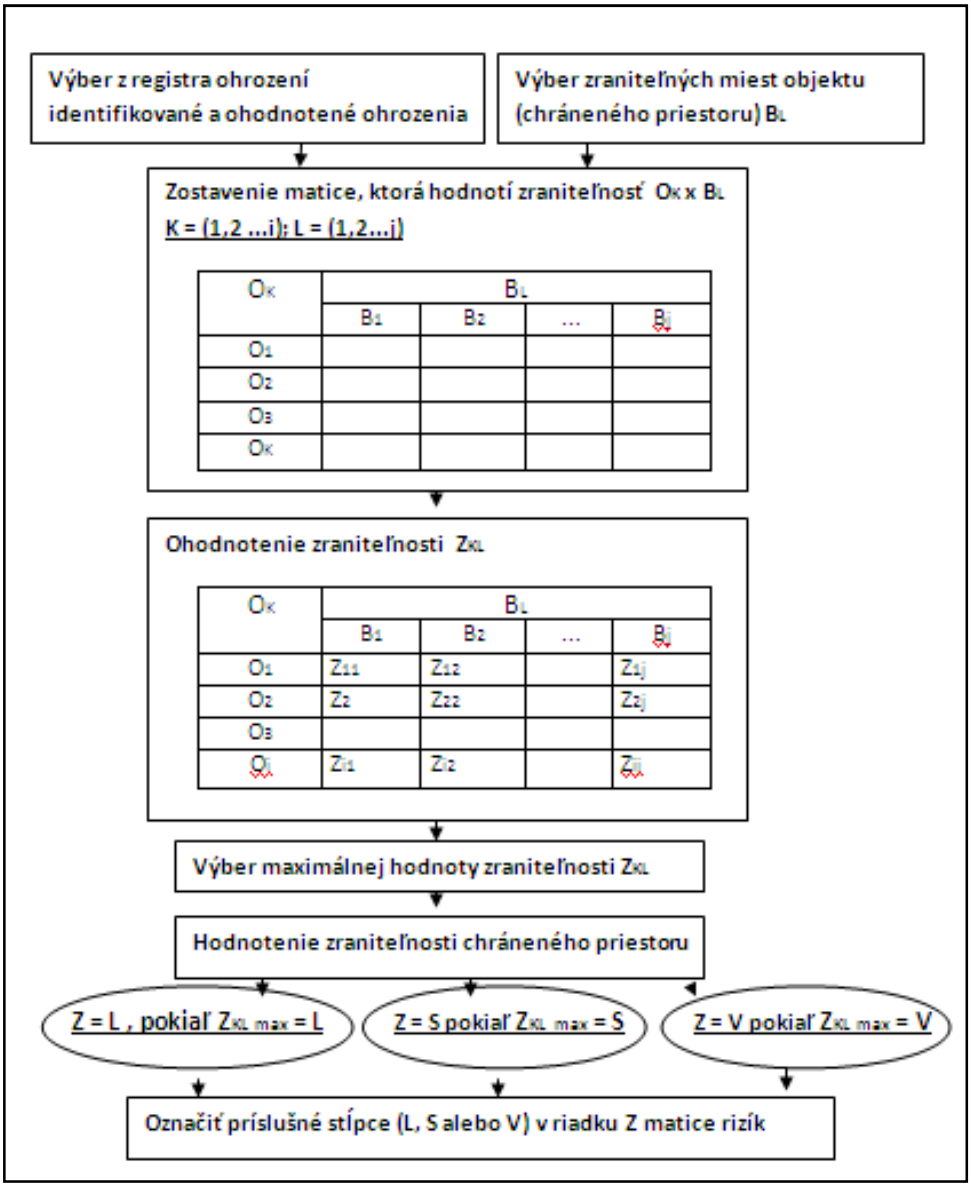


Obrázok 22 Algoritmus analýzy rizík [2]

3.2 Hodnotenie zraniteľnosti

Zraniteľnosť chráneného priestoru je vyjadrenie s akou možnosťou:

- môžu byť časti nášho chráneného priestoru, akými sú stavebné prvky, či otvorové výplne, alebo prvky systému ochrany objektu ako sú napríklad MZS, EZS, režimové opatrenia, prekonané identifikovateľným ohrozením,
- môžu byť zamestnanci, príslušníci FO, nápomocní útočníkovi k neoprávnenému prístupu k utajovaným skutočnostiam,
- môže byť manipulácia s utajovanými skutočnosťami zneužitá na získanie prístupu k utajovaným skutočnostiam,
- môže ohrozenie narušiť bezpečnosť chráneného priestoru. [2]



Obrázok 23 Algoritmus hodnotenia zraniteľnosti chráneného priestoru [2]

3.2.1 Zraniteľné miesta chráneného priestoru

Medzi zraniteľné miesta chráneného objektu môžeme považovať tieto:

- okolie, perimeter objektu, prístupy k chránenému priestoru,
- stavebné prvky objektu ako sú: steny, strechy, podlahy, stropy,
- otvorové výplne chráneného priestoru: okná, dvere, balkónové dvere, vetracie a technologické otvory,
- fyzická ochrana objektu,

- zamestnanci a cudzie osoby: návštevy, servisné služby, dodávatelia. [2]

3.2.2 Identifikovateľné ohrozenia

Medzi identifikovateľné ohrozenia sa vyberajú ohrozenia z registra ohrození, ktoré boli hodnotené minimálne ako malé(M).

Napr.:

- náhodný vlamač,
- vlamač po príprave,
- teroristi,
- pracovníci FO,
- požiar v objekte
- zahraničné spravodajské služby
- zdroj plynu v objekte. [2]

3.2.3 Matica hodnotenia zraniteľnosti

Matica ma tvar K x L, kde:

- K = množstvo ohrození, ktorých veľkosť musí byť minimálne malá (M),
- L = množstvo tried zraniteľných miest, [2]

Príklad Matice hodnotenia zraniteľnosti:

O_K	Bezpečnostné opatrenia - B_L			
	B_1	B_2	...	B_4
O_6	$Z_{6,1}$			$Z_{6,4}$
O_7				
O_8				
O_{28}	$Z_{28,1}$			$Z_{28,4}$

Obrázok 24Matica hodnotenia zraniteľnosti [2]

3.2.4 Ohodnotenie zraniteľnosti

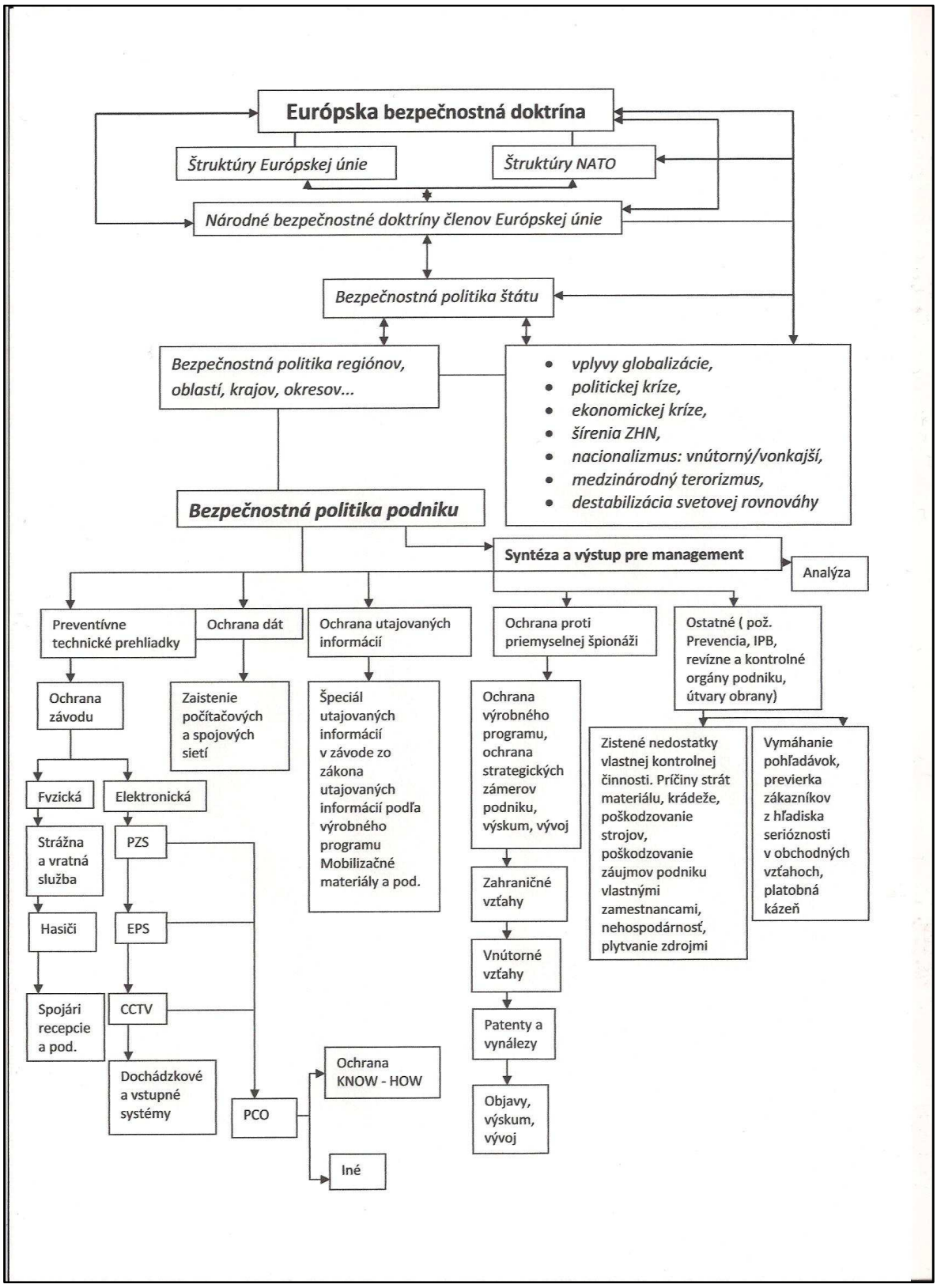
Ohodnotenie zraniteľnosti vyjadruje výšku možností ohrozenia bezpečnosti chráneného priestoru a utajovaných skutočností.

Zraniteľnosť môže byť ohodnotená nasledujúcimi stupňami:

- malá zraniteľnosť – ak neexistuje takmer žiadna možnosť na ohrozenie objektu, osôb nachádzajúcich sa v objekte alebo utajovaných skutočností, zraniteľným miestom,
- stredná zraniteľnosť – ak existuje nejaká možnosť ohrozenia objektu, osôb nachádzajúcich sa v objekte alebo utajovaných skutočností, zraniteľným miestom,
- veľká zraniteľnosť – ak je vysoká pravdepodobnosť ohrozenia objektu, osôb nachádzajúcich sa v objekte alebo utajovaných skutočností, zraniteľným miestom.

Takto ohodnotené zraniteľnosti sa zapisujú do Matice hodnotenia zraniteľnosti. [2]

3.3 Bezpečnostná politika podniku



Obrázok 25 Európska bezpečnostná doktrína a bezpečnostná politika podniku

Bezpečnostná politika je základným pilierom fungovania každého podniku. Stanovenie koncepcie bezpečnostnej politiky podniku je súčasťou riadiacich dokumentov podniku. Zahŕňa v sebe riadiace a organizačné pravidlá, normy, pokyny, nariadenia, ktoré slúžia na maximálnu ochranu podniku proti kriminálnym ale aj nekriminálnym javom a činnostiam, ktoré ohrozujú stabilnú, bezproblémovú prevádzku podniku. Tiež zahŕňa všetky stránky bezpečnosti organizácie a podporuje ostatné politiky podniku. Dokument bezpečnostnej politiky podniku obsahuje aj informácie o ohrozeniach podniku, o bezpečnostných, odborných, obchodných a prevádzkových rizikách.„*V podstatě jde o soubor organizačně řídících opatření, norem, standardů, pravidel chování s cílem zajistit bezpečnost organizace (podniku).*“(JUDr. Laucký, 2010),

Stratégia organizácie definuje hlavné ciele podniku v rámci podnikania a účasti v hospodárskej súťaži a určuje hlavné nástroje a prostriedky, ktoré napomáhajú k dosiahnutiu cieľa. Jeden z prostriedkov, ktorý umožňuje organizáciám dosahovať ich obecné ciele je presne formulovaná a následne realizovaná bezpečnostná politika organizácie. Bezpečnostná politika rozhoduje o hodnotách, záujmoch a prvkoch, ktoré chce podnik prvorado chrániť. Tiež môžeme bezpečnostnú politiku chápať ako základné pravidlo, zákon podniku, či organizácie. Bezpečnostná politika organizácie sa stáva bezpečnostnou normou podniku, či firmy.

Bezpečnosť podniku môžeme rozdeliť do troch skupín:

- obecná bezpečnosť v sebe zahŕňa predovšetkým ochranu verejného poriadku v chránenom objekte, tiež zaistenie prístrojov, zariadení, tovaru a zásob, fyzickou a režimovou ochranou,
- zvláštna bezpečnosť zaisťuje ochranu dát, počítačových a spojových sietí. Zameriava sa na ochranu výrobného programu, know– how, či priemyselnej špionáže,
- špeciálna ochrana pojednáva o zaistenie bezpečnosti použitím technických prostriedkoch k ochrane majetku a osôb. Hovoríme o poplachových zabezpečovacích signalizácií, elektronických požiarnych signalizácií, elektrickej ochrane tovaru, elektronickej kontrole vstupu a iných. [1], [9], [10]

3.3.1 Dokument bezpečnostnej politiky podniku

Dokument bezpečnostnej politiky podniku, je nosný dokument pre fungovanie každej organizácie. Tento interný riadiaci akt vyjadruje vôľu vedenia každého podniku v oblasti komplexnej ochrany organizácie. Je dôležité aby bol vždy okamžite k dispozícií, pri vzniku mimoriadnych udalostí alebo krízových situácií. *„Bezpečnostní politika by neměla být vždy jasná a transparentní, čímž vytváří image zdravého, stabilního podniku, zprůhledňuje jeho cíle v oblasti bezpečnosti a samotného podnikání.*“(JUDr. Laucký, 2010)

Základný dokument bezpečnostnej politiky podniku môže obsahovať:

- program, ktorý pojednáva o informačnej bezpečnosti podniku jeho ciele zamerané na informačnú bezpečnosť,
- zodpovednosť za plnenie bezpečnostnej politiky podniku,
- prostriedky k dodržiavaniu bezpečnostnej politiky podniku,
- hlavné zásady k dodržiavaniu politiky,
- hlavné zásady koordinácie majetkovej, osobnej a informačnej bezpečnosti v organizácií.

Zodpovedané by mali byť aj tieto otázky:

- kto nesie zodpovednosť za naplnenie záverov bezpečnostnej politiky,
- ktorých oblastí činnosti organizácie sa dotýka bezpečnostná politika,
- aký je časový horizont pre naplnenie cieľov bezpečnostnej politiky,
- spôsob zavádzania bezpečnostnej politiky do praxe,
- aké sú kladené požiadavky na bezpečnostnú politiku z hľadiska nákladov a efektivity,
- ako sa bude trestať porušenie dodržiavania bezpečnostnej politiky,
- zásady koordinovania osobnej, majetkovej a informačnej bezpečnosti organizácie.

Dokumenty, ktoré obsahujú hlavné zásady bezpečnostnej politiky:

- špecifikácie platných predpisov a iných oprávnení,
- bezpečnostné požiadavky podniku,
- spôsob ochrany informačných systémov vo fyzickej organizačnej a softwarovej oblasti,
- postupy a spôsoby riešení,
- základné zásady riešení bezpečnostných situácií,

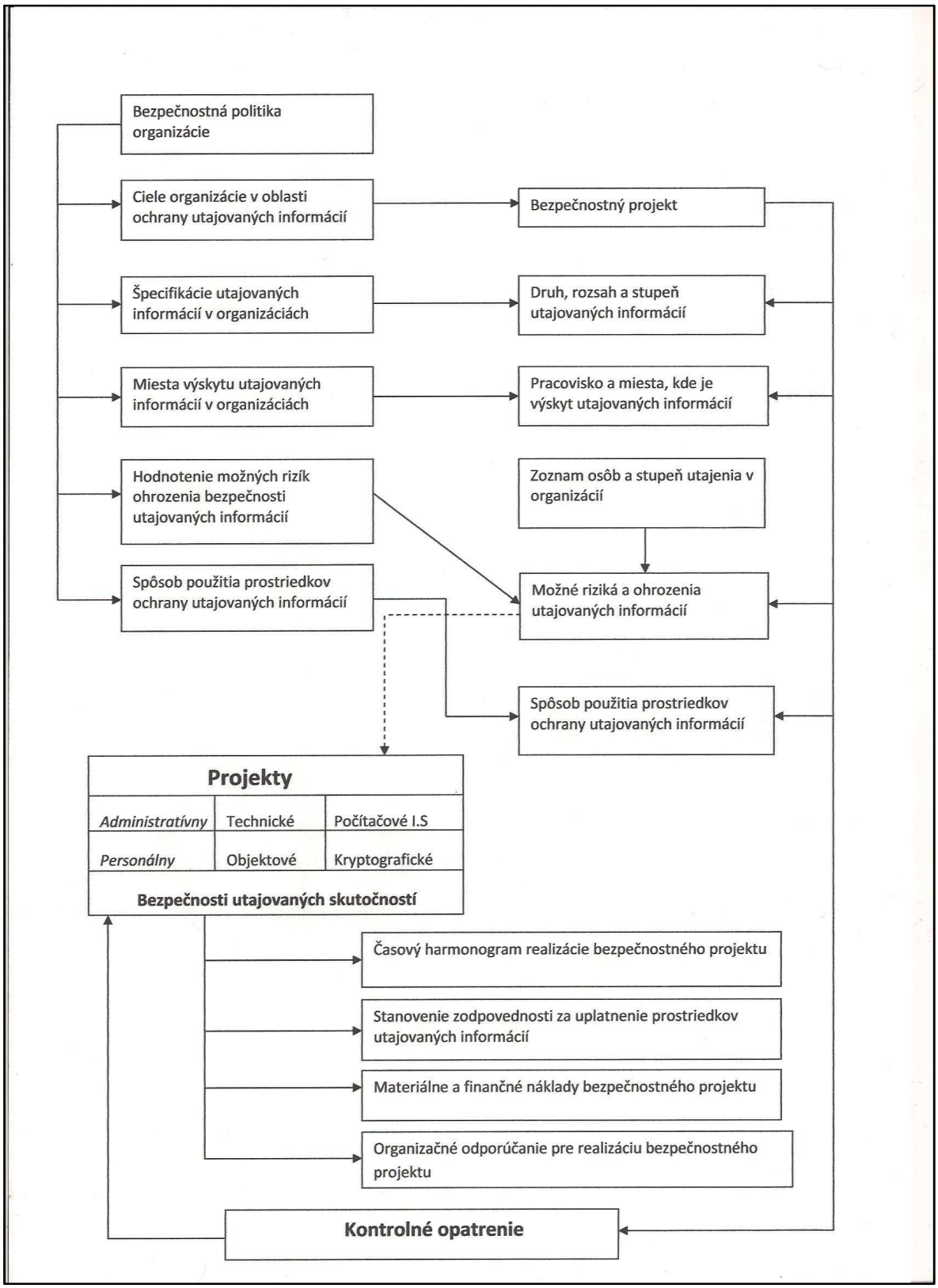
- spôsoby a metódy spolupráce informačnej bezpečnosti podniku s osobnou a majetkovou bezpečnosťou podniku.

Oblasť záujmov bezpečnostnej politiky:

- politika administratívnej bezpečnosti,
- politika personálnej bezpečnosti,
- politika objektovej bezpečnosti,
- politika ochrany majetku,
- politika ochrany nehmotného majetku,
- politika technickej bezpečnosti,
- politika ochrany utajovaných informácií,
- politika bezpečnosti informačných systémov,
- politika kryptografickej ochrany.

Tvorba bezpečnostnej politiky a bezpečnostného projektu podnikov nie je mechanická práca, kde sa prvky dosadzujú do vopred vypracovanej šablóny, ale ide o tvorivú činnosť riešenia daného problému špecifických podmienok konkrétnej organizácie. [3], [9], [10]

3.4 Bezpečnostný projekt



Obrázok 26 Schéma bezpečnostného projektu

„Bezpečnostní projekt představuje nezbytnou dokumentaci (písemnou i grafickou) důvěryhodného, účinného a efektivního systému zabezpečení ochrany bezpečnostních zájmů příslušného konkrétního podnikatelského subjektu nebo jeho organizačních částí.“(JUDr. Brabec, 1996)

Bezpečnostný projekt je významná súčasť dokumentácie bezpečnostného zaistenia ochrany každého objektu, kde je navrhnutá bezpečnostná politika. Bezpečnostný projekt odpovedá na otázky zabezpečenia a bezpečnostnej ochrany objektu. Je predovšetkým plán pre realizáciu vybraných najvýhodnejší protiopatrení a nástroj pre vytvorenie bezpečnostnej štruktúry podniku. Vychádza zo schválených záverov a poznatkov bezpečnostnej analýzy a musí byť v súlade s bezpečnostnou politikou.

Bezpečnostný projekt prezentuje bezpečnostné ciele a navrhuje konkrétne postupy ich realizácie. Podstata projektu je poukázanie na pravdepodobné hroziace riziká, ich charakter, časové možnosti pôsobenia a miera odhadovaného ohrozenia. Najvýznamnejšou časťou bezpečnostného projektu je štruktúra krízového managementu.

Oblasti bezpečnostného projektu:

- administratívna,
- personálna,
- technická,
- informačných systémov,
- objektová,
- organizačná,
- prevádzková.

K vypracovaniu bezpečnostného projektu je potrebné vykonať dve samostatné etapy:

- vypracovanie projektovej štúdie realizácie,
  - definovanie problému,
  - dve varianty návrhu riešenia,
  - odôvodnené odporúčanie najvhodnejšej varianty.
- spracovanie projektu,
  - návrh riešenia schválenej verzie,
  - časový plán realizácie,
  - zdôvodnený návrh pre výber dodávateľa,
  - materiálne a finančné požiadavky,

- organizačné odporúčania pre realizáciu projektu.

V úvodnej časti projektu je prezentácia pravdepodobných rizík, ich charakter, časové alternatívy pôsobenia a rozmer predpokladaného ohrozenia. V druhej časti je určená úprava organizačnej štruktúry krízového vedenia, spôsob riadenia a právomoci. Ďalšie časti projektu potom riešia bezpečnostné otázky, časové harmonogramy realizácie, spôsoby prevedenia ochrany, spôsob pri vykonávaní a ohraničení povinností a zodpovedností. V poslednej časti ide o konkretizáciu podniku, predovšetkým o programy normalizácie a revitalizácie. [3], [6]

3.4.1 Bezpečnostné dokumenty

Hlavné nástroje pre vykonanie bezpečnostnej politiky sú bezpečnostné dokumenty. Podnikové nariadenia vychádzajú zo zákonných ustanovení štátnej správy, odborných útvarov podniku, strategických potrieb podniku a potrieb obchodných partnerov podniku. Tieto dokumenty sú spracované ako podnikové smernice, ktoré obsahujú pokyny, nariadenia, popis náplní a pracovných postupov. Hlavným cieľom bezpečnostných dokumentov je prevencia hrozieb a rizík.

Dokument hovorí o tom:

- kto má robiť,
- čo má robiť,
- ako to má robiť,
- kedy to má robiť.

Prehľad bezpečnostných dokumentov:

- prehľad o rizikových miestach objektu,
- rozhodnutie o zásadách bezpečnostnej politiky podniku,
- smernice pre výkon strážnej služby,
- poriadok návštev,
- poriadok vjazdu a parkovania vozidiel v objekte,
- pravidlá pre prepravu cenností a ich doprovod,
- dokumenty o prevádzke a inštalácií zabezpečovacích a protipožiarnych systémoch,
- zásady režimových opatrení. [9]

3.5 Zákon o ochrane utajovaných informácií

Pre porovnanie som vybrala úryvky zo zákonov o ochrane utajovaných informácií v Slovenskej republike a v Českej republike.

3.5.1 215/2004 Zákon o ochrane utajovaných skutočností v SR

215/2004 Zákon o ochrane utajovaných skutočností v SR hovorí:

§ 1 Predmet úpravy

(1) „Tento zákon upravuje podmienky na ochranu utajovaných skutočností, práva a povinnosti právnických osôb a fyzických osôb pri tejto ochrane, pôsobnosť Národného bezpečnostného úradu (ďalej len "úrad") a pôsobnosť ďalších štátnych orgánov vo vzťahu k utajovaným skutočnostiam a zodpovednosť za porušenie povinností ustanovených týmto zákonom.

(2) Tento zákon sa nevzťahuje na ochranu tajomstva upraveného v osobitných predpisoch. 1)“

§ 2 Základné pojmy

„Na účely tohto zákona je:

a) utajovanou skutočnosťou informácia alebo vec určená pôvodcom utajovanej skutočnosti, ktorú vzhľadom na záujem Slovenskej republiky treba chrániť pred vyzradením, zneužitím, poškodením, neoprávneným rozmnožením, zničením, stratou alebo odcudzením (ďalej len "neoprávnená manipulácia") a ktorá môže vznikať len v oblastiach, ktoré ustanoví vláda Slovenskej republiky svojím nariadením,

b) informáciou

1. obsah písomnosti, nákresu, výkresu, mapy, fotografie, grafu alebo iného záznamu,

2. obsah ústneho vyjadrenia,

3. obsah elektrického, elektromagnetického, elektronického alebo iného fyzikálneho transportného média,

c) vecou

1. hmotný nosič so záznamom informácií,

2. výrobok,

3. zariadenie,

4. nehnuteľnosť,

d) ujmou také ohrozenie alebo poškodenie záujmov Slovenskej republiky alebo záujmu, ku ktorého ochrane sa Slovenská republika zaviazala, ktorého následky nemožno odstrániť alebo možno ich zmierniť iba následným opatrením; podľa významu záujmu a závažnosti spôsobenej ujmy sa ujma člení na mimoriadne vážnu ujmu, vážnu ujmu, jednoduchú ujmu a nevýhodnosť pre záujmy Slovenskej republiky,

e) pôvodcom utajovanej skutočnosti právnická osoba alebo fyzická osoba, ktorá je oprávnená rozhodnúť, že informácia podľa písmena b) alebo vec podľa písmena c) je utajovanou skutočnosťou, určiť stupeň utajenia a rozhodnúť o zmene alebo zrušení stupňa jej utajenia,

f) oprávnenou osobou právnická osoba alebo fyzická osoba, ktorá je určená na oboznamovanie sa s utajovanými skutočnosťami alebo ktorej oprávnenie na oboznamovanie sa s utajovanými skutočnosťami vzniklo zo zákona,

g) nepovolanou osobou fyzická osoba, ktorá nie je oprávnená oboznamovať sa s utajovanými skutočnosťami alebo ktorá nie je oprávnená oboznamovať sa s utajovanými skutočnosťami nad rozsah, ktorý jej je určený,

h) cudzou mocou cudzí štát, orgány cudzieho štátu alebo organizácie, ktoré cudzí štát používa na riadenie alebo vykonávanie svojej moci a činnosti; cudzou mocou sú aj nadštátne organizácie, medzinárodné organizácie a združenia štátov,

i) technickým prostriedkom zariadenie alebo systém určený na vytváranie, spracúvanie, prenos, ukladanie a ochranu utajovaných skutočností,

j) certifikáciou činnosť, ktorou sa overuje a osvedčuje, či technický prostriedok, prostriedok šifrovej ochrany informácií, mechanický zábranný prostriedok alebo technický zabezpečovací prostriedok je spôsobilý chrániť utajované skutočnosti,

k) autorizáciou poverenie štátneho orgánu alebo právnickej osoby na vykonávanie činnosti pri certifikácii,

l) certifikačnou autoritou výkon funkcie spojenej s vydávaním a overovaním digitálnych certifikátov verejných kľúčov používaných v asymetrických šifrových systémoch,

m) digitálnym certifikátom elektronické potvrdenie slúžiace na priradenie verejného podpisového kľúča ku konkrétnemu subjektu a potvrdzujúce jeho identitu,

n) verejným podpisovým kľúčom kryptografický kľúč využívaný na overenie elektronického podpisu,

o) systém šifrovej ochrany informácií súbor prostriedkov šifrovej ochrany informácií spolu s celou infraštruktúrou na generovanie, distribúciu a likvidáciu šifrových materiálov po skončení ich platnosti,

p) prostriedkom šifrovej ochrany informácií zariadenie určené na šifrovú ochranu informácií a šifrové materiály,

q) objektom budova alebo iný stavebne alebo inak ohraničený priestor, v ktorom sa nachádzajú chránené priestory,

r) chráneným priestorom stavebne alebo inak ohraničený priestor vo vnútri objektu, ktorý je určený naukladanie a manipuláciu s utajovanými skutočnosťami, zodpovedajúci príslušnému stupňu utajenia,

s) mechanickým zábranným prostriedkom je zariadenie alebo systém slúžiaci na zabránenie prístupu nepovolaným osobám,

t) technickým zabezpečovacím prostriedkom je zariadenie alebo systém informujúci o stave a narušení objektu alebo chráneného priestoru.“

§ 3 Stupne utajenia

a) „Utajované skutočnosti sa podľa stupňa utajenia členia na
a) prísne tajné,
b) tajné,
c) dôverné,
d) vyhradené.

b) Stupne utajenia sa označujú slovami "Prísne tajné", "Tajné", "Dôverné" a "Vyhradené" alebo skratkami "PT", "T", "D" a "V".

c) Stupňom utajenia Prísne tajné sa označuje utajovaná skutočnosť vtedy, ak by následkom neoprávnenej manipulácie s ňou mohlo byť vážne ohrozené zachovanie ústavnosti, zvrchovanosti a územnej celistvosti štátu alebo by mohli vzniknúť nenahraditeľné a vážne škody v oblasti obrany, bezpečnosti, ekonomických záujmov, zahraničnej politiky alebo medzinárodných vzťahov, a tým mohla vzniknúť mimoriadne vážna ujma na záujmoch Slovenskej republiky.

d) Stupňom utajenia Tajné sa označuje utajovaná skutočnosť vtedy, ak by následkom neoprávnenej manipulácie s ňou mohlo byť ohrozené zahraničnopolitické postavenie, obrana, bezpečnosť a záujmy štátu v medzinárodnej a ekonomickej oblasti, a tým by mohla vzniknúť vážna ujma na záujmoch Slovenskej republiky.

e) Stupňom utajenia Dôverné sa označuje utajovaná skutočnosť vtedy, ak by následkom neoprávnenej manipulácie s ňou mohlo dôjsť k poškodeniu štátnych záujmov, verejných záujmov alebo právom chránených záujmov štátneho orgánu, a tým k jednoduchej ujme na záujmoch Slovenskej republiky.

f) Stupňom utajenia Vyhradené sa označuje utajovaná skutočnosť vtedy, ak by neoprávnená manipulácia s ňou mohla zapríčiniť poškodenie právom chránených záujmov právnickej osoby alebo fyzickej osoby, ktoré by mohlo byť nevýhodné pre záujmy Slovenskej republiky.“

§ 15 Bezpečnostná previerka navrhovanej osoby:

(1) „Bezpečnostnou previerkou sa zisťuje, či navrhovaná osoba spĺňa predpoklady uvedené v § 10 ods. 1 na oboznamovanie sa s utajovanými skutočnosťami.

(2) Podľa stupňa utajenia sa vykonáva

a) bezpečnostná previerka I. stupňa pre stupeň utajenia Vyhradené,

b) bezpečnostná previerka II. stupňa pre stupeň utajenia Dôverné,

c) bezpečnostná previerka III. stupňa pre stupeň utajenia Tajné,

d) bezpečnostná previerka IV. stupňa pre stupeň utajenia Prísne tajné.„ [21]

3.5.2 412/2005 Zákon o ochrane utajovaných informácií a o bezpečnostnej spôsobilosti v ČR

412/2005 Zákon o ochrane utajovaných informácií a o bezpečnostnej spôsobilosti v ČR hovorí:

§ 1 Predmet úpravy

„ Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a dalš ípožadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.“

§ 2 Vymedzenie pojmov

„ Pro účely tohoto zákona serozumí:

a) utajovanou informací informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může bý tpro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací (§ 139),

b) zájmem České republiky zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob,

c) porušením povinnosti při ochraně utajované informace porušení povinnosti uložené tímto zákonem nebo na základě tohoto zákona,

d) orgánem státu organizační složka státu podle zvláštního právního předpisu 1), kraj 2), hlavní město Praha 3), městská část hlavního města Prahy a obec 4) při výkonu státní správy vevěcech, které stanoví zvláštní právní předpis; orgánem státu se rozumí i Bezpečnostní informační služba 5), Vojenské zpravodajství 6) a Česká národní banka 7),

e) odpovědnou osobou,

1. *u ministerstva ministr,*
2. *u jiného ústředního správního úřadu ten, kdo stojí v jeho čele,*
3. *u organizační složky státu, zřízené jinou organizační složkou státu, ten, kdo je odpovědnou osobou u organizační složky státu vykonávající funkci jejího zřizovatele,*
4. *u dalších organizačních složek státu ten, kdo stojí v jejich čele,*
5. *u Bezpečnostní informační služby a Vojenského zpravodajství ředitel,*
6. *u České národní banky guvernér,*
7. *u kraje ředitel krajského úřadu,*
8. *u hlavního města Prahy ředitel Magistrátu hlavní homěsta Prahy,*
9. *u městské části hlavního města Prahy tajemník úřadu městské části, a není-li jej, starosta městské části,*
10. *u statutárního města tajemník magistrátu,*
11. *u dalších měst a obcí tajemník jejich úřadu, a není-li jej, starosta,*
12. *u organizační složky územního samosprávného celku ten, kdo je odpovědnou osobou u územního samosprávného celku vykonávajícího funkci jejího zřizovatele,*

13. u právnických osob neuvedených v bodech 6 až 11 statutární orgán; jedná-li podle zvláštního právního předpisu 8) jménem těchto jiných právnických osob více osob, které jsou statutárním orgánem, nebo osoba, která statutárním orgánem není, pak je odpovědnou osobou pouze ta z nich, která je jednáním ve věcech upravených tímto zákonem pověřena, a

14. podnikající fyzická osoba 9),

f) původcem utajované informace orgán státu, právnická osoba nebo podnikající fyzická osoba, u nichž utajovaná informace vznikla, nebo Úřad průmyslového vlastnictví podle § 70 odst. 4,

g) cizí mocí cizístát nebo jeho orgán a nebo nadnárodní nebo mezinárodní organizace nebo její orgán,

h) neoprávněnou osobou fyzická nebo právnická osoba, která nesplňuje podmínky přístupu k utajované informaci stanovené tímto zákonem,

i) poučením písemný záznam o seznámení fyzické osoby s jejími právy a povinnostmi v oblasti ochrany utajovaných informací a s následky jejich porušení,

j) bezpečnostním standardem utajovaný soubor pravidel, ve kterém se stanoví postupy, technická řešení, bezpečnostní parametry a organizační opatření pro zajištění nejmenší možné míry ochrany utajovaných informací,

k) bezpečnostním provozním módem prostředí, ve kterém informační systém pracuje, charakterizované stupněm utajení zpracovávané utajované informace a úrovněmi oprávnění uživatelů.“

§ 4 Stupne utajenia

„Utajovaná informace se klasifikuje stupněm utajení

a) Přísně tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobi tmimořádně vážnou újmu zájmům České republiky,

b) Tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,

c) Důvěrné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,

d) Vyhrazené, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné prozájmy České republiky.“

O bezpečnostnej previerke hovorí § 157

„ 8) Souhlas s určením navrhované osoby bez předchozího provedení bezpečnostní prověrky, který byl vydán podle dosavadních právních předpisů, se po dobu 6 měsíců ode dne nabytí účinnosti tohoto zákona považuje za souhlas s jednorázovým přístupem k utajované informaci pro stupeň utajení, prokterý má být navrhované osobě vydáno osvědčení.

18) Bezpečnostní prověrka zahájená přede dnem nabytí účinnosti tohoto zákona se dokončí podle dosavadních právních předpisů. Na její dokončení se vztahuje lhůta pro provedení srovnatelného řízení o vydání osvědčení podle tohoto zákona s tím, že lhůta začíná běžet ode dne nabytí účinnosti tohoto zákona.

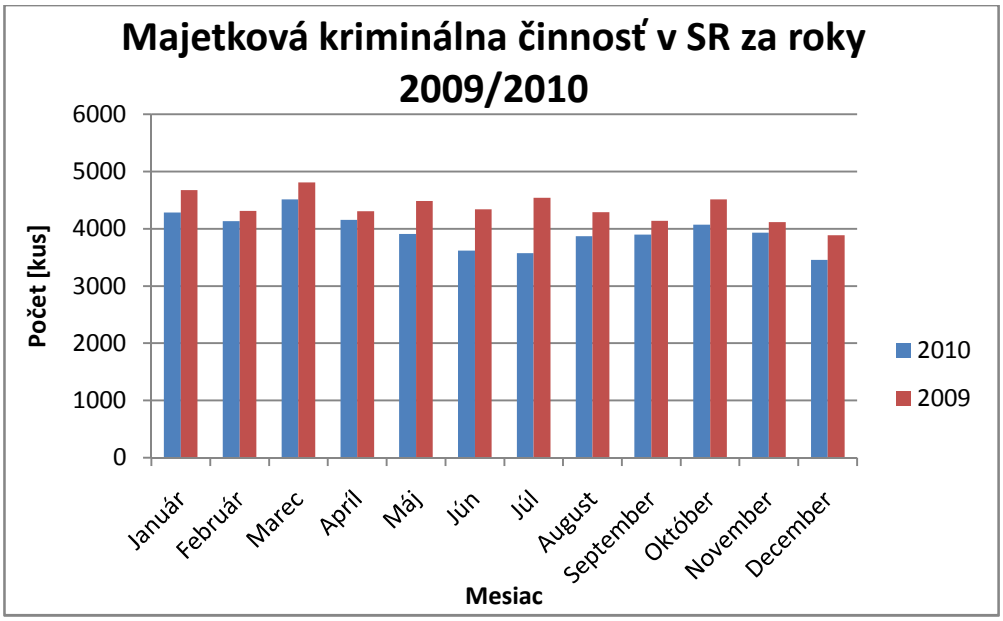
28) Provedení bezpečnostní prověrky fyzické osoby, bezpečnostní prověrky organizace, certifikace technického prostředku, certifikace informačního systému, certifikace kryptografického prostředku, ověření bezpečnostní způsobilosti fyzické osoby, vydání certifikátu potvrzující cizí moci, že navrhované osobě bylo vydáno osvědčení nebo organizaci potvrzení, a vydání souhlasu s poskytováním utajovaných informací meziorganizací a zahraničním partnerem seřídí dosavadními právními předpisy pouze tehdy, jestliže žádost byla předána k poštovní přepravě nebo jinak doručena či podána nejpozději 45 dnů předednem nabytí účinnosti tohoto zákona.“ [22]

II. PRAKTICKÁ ČASŤ

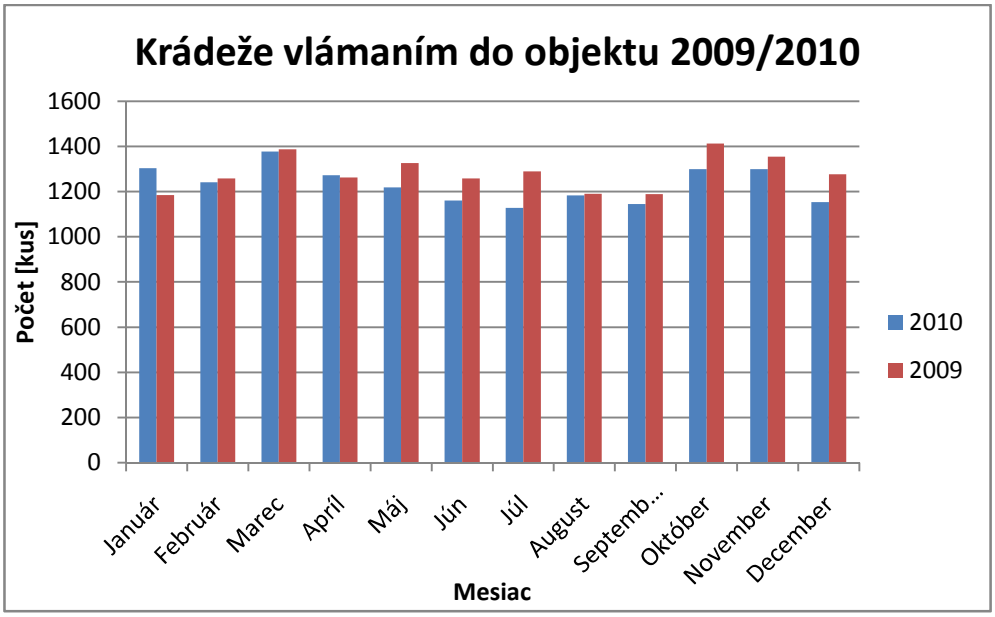
4 SÚČASTNÝ STAV OBJEKTOVEJ BEZPEČNOSTI V SLOVENSKEJ REPUBLIKE

4.1 Štatistika kriminality v Slovenskej republike

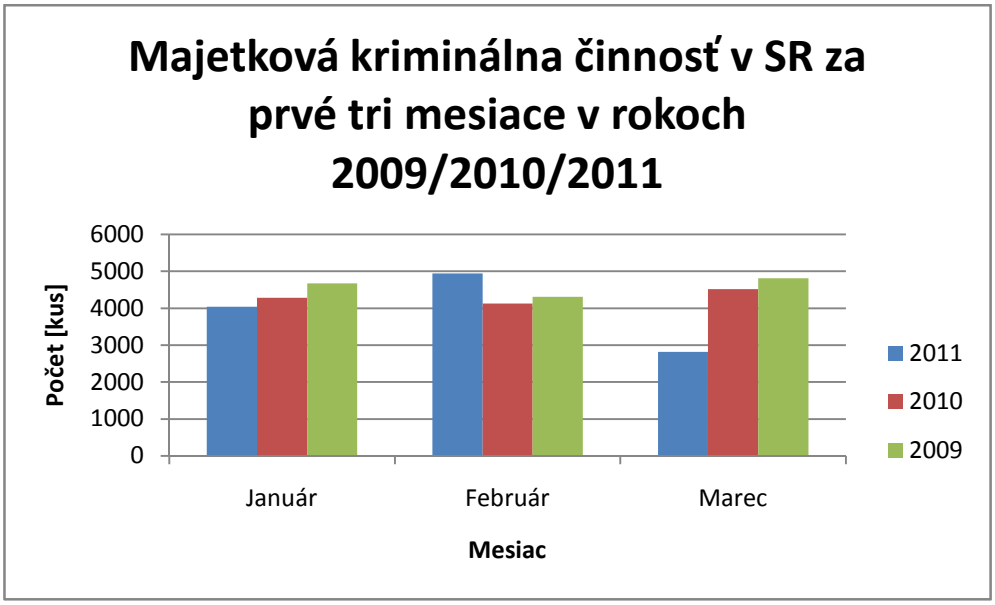
Štatistika kriminality objektovej bezpečnosti v Slovenskej republike mala za rok 2010, v porovnaní s predchádzajúcimi rokmi klesavú tendenciu. Podľa informácií dostupných na stránkach národného bezpečnostného úradu som zhotovila grafy, ktoré tento fakt potvrdzujú. Za prvé tri mesiace roku 2011 sa dá povedať, že majetková kriminálna činnosť v Slovenskej republike nestúpa, práve naopak. Je už len na uvážení, či pokles násilných vniknutí do objektu a krádeží, súvisí s uvedomením občanov a majiteľov podnikov, že objekty si treba chrániť a s tým súvisiacich zabezpečení objektov, alebo je to tým, že počet kriminálnikov ubúda?



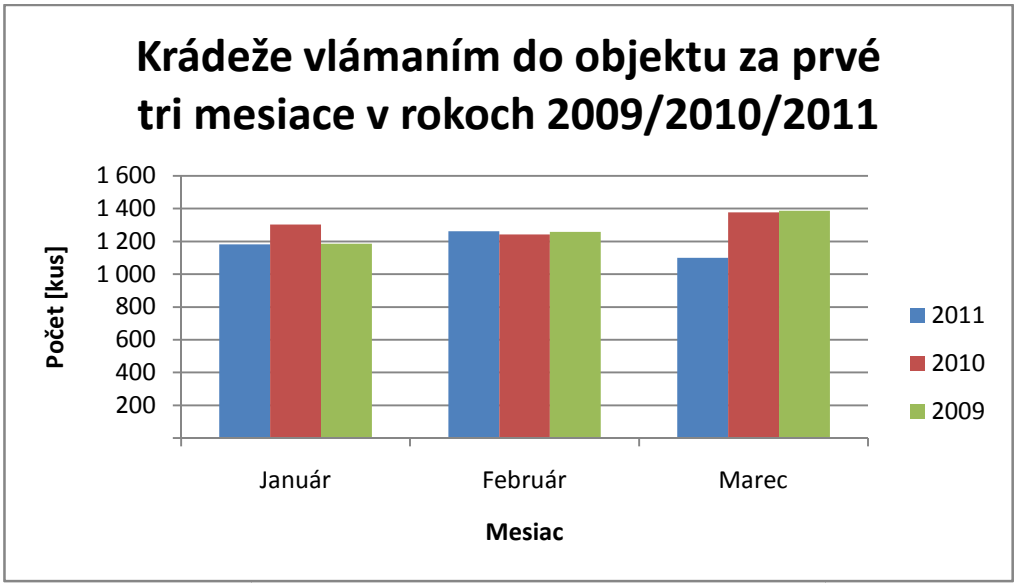
Obrázok 27 Majetková kriminálna činnosť v SR za roky 2009/2010



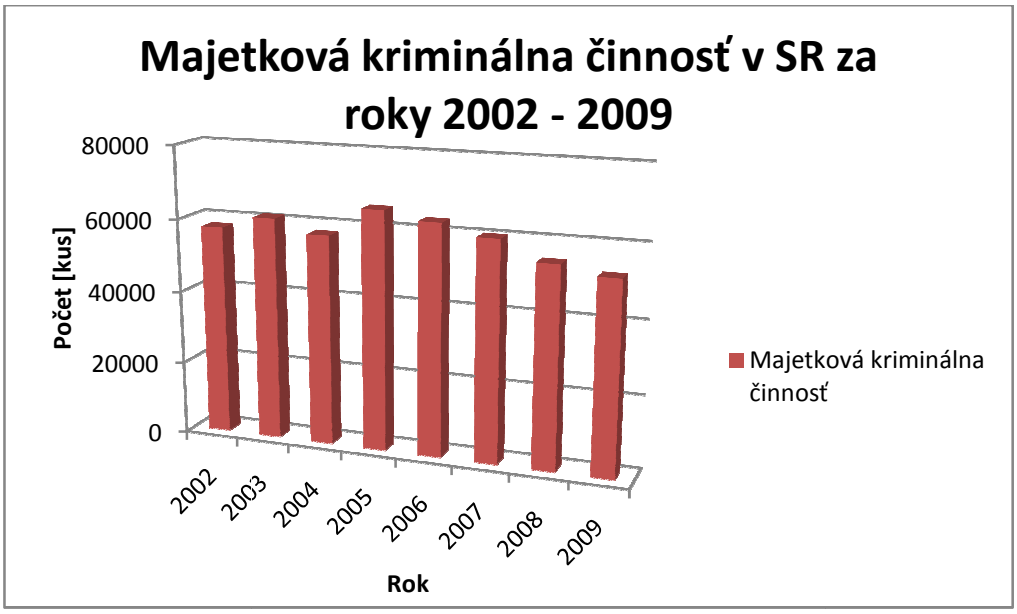
Obrázok 28 Krádeže vlámaním do objektu 2009/2010



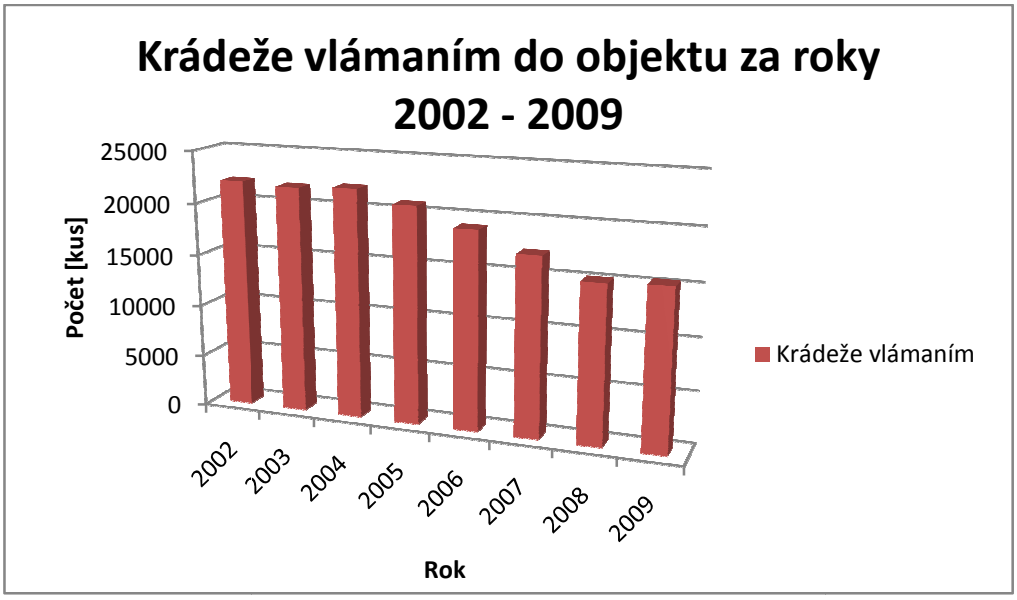
Obrázok 29 Majetková kriminálna činnosť v SR za prvé tri mesiace v rokoch 2009/2010/2011



Obrázok 30 Krádeže vlámaním do objektu za prvé tri mesiace v rokoch 2009/2010/2011



Obrázok 31 Majetková kriminálna činnosť v SR za roky 2002 - 2009



Obrázok 32 Krádeže vlámaním do objektu za roky 2002 – 2009

4.2 Koncepcia ochrany utajovaných skutočností Ministerstva vnútra Slovenskej republiky

Plán štruktúry ochrany utajovaných skutočností Ministerstva vnútra Slovenskej republiky je skonštruovaný v súlade s platnou legislatívou:

- zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- uznesenie vlády Slovenskej republiky č. 475 z 30. mája 2007 k návrhu koncepcie ochrany utajovaných skutočností v Slovenskej republike, ktorú vypracoval Národný bezpečnostný úrad.

Cieľom koncepcie ochrany utajovaných skutočností je vytvoriť požadované štádium bezpečnosti utajovaných skutočností na základe optimálnosti flexibility a homogénnosti systému ochrany utajovaných skutočností. Prioritou je zachovanie funkčnosti systému pri minimálnych nákladoch, pružnosti reakcie na zmeny hrozieb a bezpečnostných rizík a harmonizácie princípov, terminológie, metodík a postupov posudzovania bezpečnostných rizík.

Osnova ochrany utajovaných skutočností vychádza z ich aktuálneho stavu v rezorte ministerstva vnútra a z oboznámením sa so zabezpečením v oblasti:

- personálnej bezpečnosti,

- priemyselnej bezpečnosti,
- administratívnej bezpečnosti,
- informačnej bezpečnosti,
- objektovej a fyzickej bezpečnosti,
- šifrovej ochrany informácií.

4.2.1 Fyzická bezpečnosť a objektová bezpečnosť

Platná legislatíva:

- vyhláška NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení vyhlášky NBÚ č. 315/2006 Z. z.,
- vyhláška NBÚ č. 337/2004 Z. z., s ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní v znení vyhlášky NBÚ č. 314/2006 Z. z. a nariadením o OUS.

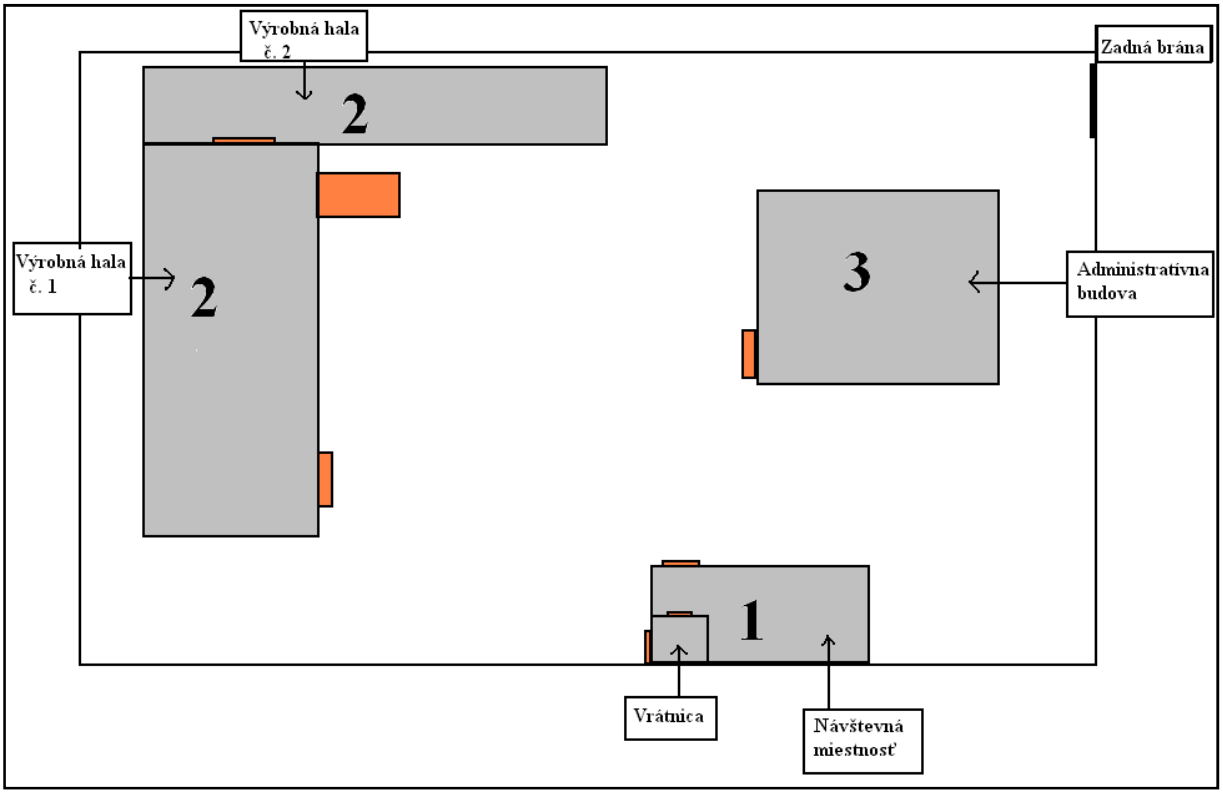
Vyhláška o fyzickej a objektovej bezpečnosti stanovuje štandard fyzickej a objektovej bezpečnosti, ktorý navrhuje a realizuje podľa zadefinovaných matematických vzorcov pre konkrétne stupne utajovania, optimálny systém na ochranu utajovaných skutočností. Na základe toho bol vypracovaný vzorový bezpečnostný koncept pre fyzickú bezpečnosť a objektovú bezpečnosť pre chránený priestor. Časť tohto dokumentu bude vložená do príloh bakalárskej práce.

Súčasný stav v oblasti fyzickej bezpečnosti a objektovej bezpečnosti pri plnení uvedeného základného cieľa je uspokojivý. Táto oblasť je ovplyvnená počtom oprávnených osôb a stupňom utajenia utajovaných skutočností. So stupňom utajovaných skutočností, ktoré treba zaistiť priamoúmerne stúpa aj náročnosť ochrany objektov. *„V minulosti bola zrealizovaná prestavba najviac používaných trezorov typu KOVONA, v dôsledku čoho nebolo potrebné zakúpiť nové trezory. Uvedený typ trezoru bol certifikovaný NBÚ do stupňa utajenia „Dôverné“. Touto certifikáciou boli ušetrené značné finančné prostriedky ministerstva vnútra na zabezpečenie OUS.“*

Písomnosti utajované stupňom utajenia Tajné a Prísne tajné sú umiestnené v chránených režimových miestnostiach, ktoré sa nazývajú REMUS I a REMUS II.

5 NÁVRHY AKTÍVNYCH REŽIMOVÝCH OPATRENÍ V PRIEMYSELNÝCH AREÁLOCH A VEĽKÝCH STRÁŽENÝCH OBJEKTOCH

5.1 Systémový návrh areálu



Obrázok 33 Systémový návrh areálu

5.2 Analýza objektu

Objekt slúžiaci na simulovanie režimových opatrení je výrobňa patentovaných súčiastok pre automobilový priemysel. V objekte sa nachádza vrátnica slúžiaca pre kontrolu vstupu osôb a automobilov. Pre vstup osôb slúži malý vchod, autá majú vyhradenú veľkú bránu. Podnik disponuje jednou výrobnou halou a administratívnou budovou, v ktorej sídli riaditeľ. Zamestnanci využívajú na vstup do výrobnej haly bezkontaktnú čipovú kartu, ktorá zároveň slúži aj ako kontrola dochádzky zamestnancov. Pre nakladanie tovaru slúži nákladná rampa. Do administratívnej budovy má povolený vstup iba management podniku. Pre návštevy je vyhradená návštevná čakacia miestnosť.

5.2.1 Rozdelenie objektu do zón

Priestory podniku sú rozdelené do troch skupín podľa oprávnenia vstupu osôb nachádzajúcich sa v areáli.

1. zóna = priestory vrátnice, návštevnej miestnosti a po obvode celého areálu. Do tejto zóny majú povolený vstup všetci zamestnanci pracujúci v podniku a legitimované návštevy s príslušným sprievodným zamestnancom.
2. zóna = výrobná hala č.1 a výrobná hala č.2, kde majú možnosť vstupovať iba zamestnanci zamestnaný v podniku vo výrobnej sfére a management podniku,
3. zóna = administratívna budova, slúžiaca výhradne pre zamestnancov managementu podniku. Ostatní zamestnanci majú povolenie vstupu iba na súhlas poverenej osoby.

5.3 Projekt bezpečnostného systému

5.3.1 Prístupový systém

Systém riadi všetky prístupové miesta do objektu a prístupové miesta do jednotlivých zón. Na základe identifikácie užívateľa vyhodnotí všetky potrebné informácie a priradí alebo nepriradí prístupové práva užívateľovi. Vstup osoby bude automaticky zaregistrovaný do databáze systému s časovým údajom.

Prevedenie: prístupový podsystém na báze bezkontaktných čipových kariet použitých v celom bezpečnostnom systéme.

Vlastnosti:

- kompletné centralizované monitorovanie dverí v reálnom čase,
- rýchla lokalizácia osôb v jednotlivých zónach objektu,
- elektrické otváranie dverí,
- jednoduché nastavenie práv užívateľov a ich zmien,
- usmernenie osôb prostredníctvom elektromechanických turniketov s definovaným smerom otáčania, aretovateľné bránky a zábradlia s funkciou „PANIC“,
- vyšší stupeň zabezpečenia prístupu na režimové pracovisko čítačkou biometrie rúk,
- fotografia zamestnanca prechádzajúceho cez dochádzkový systém sa zobrazí na monitore informátora za účelom zabrániť zneužitiu bezkontaktnej čipovej karty.

5.3.2 Dochádzkový systém

Prechody prístupovými miestami sa zaznamenávajú a uchovávajú so všetkými potrebnými údajmi o zamestnancovi a bude k nim možný centrálny aj lokálny prístup. Identifikačné zariadenie používateľa nie je priamym nositeľom osobných a prístupových informácií o užívateľovi v systéme, čím je vylúčené bezpečnostné riziko.

Prevedenie: dochádzkový systém je nadstavbou prístupového systému.

Vlastnosti:

- evidencia príchodov a odchodov pracovníkov na pracovisko pre účely kontroly dochádzky,
- návštevy sú evidované – kto, kedy a dôvod návštevy,
- evidencia neprítomnosti zamestnancov na pracovisku počas pracovnej doby z dôvodov návštevy lekára, služobnej cesty a iných,
- editácia, filtrovanie a mazanie záznamov o dochádzke

5.3.3 Návštevný systém

Návštevný systém rieši prijímanie, smerovanie a identifikáciu návštev. Návštevy sú vybavené návštevnou kartou a ich pohyb po objekte je kontrolovaný a sprevádzaný poverenou osobou. Návštevy v objekte je možné povoliť len tým osobám, ktoré sa aktuálne v objekte nachádzajú.

Prevedenie: aplikácia na báze čítačky dokladov, intranetový a informačný terminál.

Vlastnosti:

- zaznamenanie údajov do elektronickej databázy o návšteve z dokladov vyrobených podľa ICAO normy (OP, pasy, víza...),
- evidencia prítomnosti pracovníkov v objekte pre účely informátora a návštevy,

5.3.4 Kamerový systém

Objekt obsahuje je aj kamerový systém, navrhnutý s analógovými alebo digitálnymi kamerami.

Prevedenie: kamerový systém na báze analógových alebo digitálnych kamier a úložiska pre nahrávanie záznamu.

Vlastnosti:

- záznam nahrávania sa uchováva minimálne 7 dní,
- obsluha má možnosť výberu druhu nahrávania,
- prístup k záznamom cez LAN,
- záznamy sú archivované (DVD – RW, Blue-Ray, HDD) a je možné ich spätne vyhľadať podľa dátumu a času,
- videosignály je možné sledovať z kamier v priestoroch strážnej služby,
- videozáznamy sa ukladajú do predarchívnej starostlivosti (páskové knižnice, diskové polia) na minimálne 6 mesiacov.

5.3.5 Mechanické zábranné prostriedky

Všetky mechanické zábrany v interiéri aj v exteriéri sú vyhotovené z nekorodujúceho materiálu s reprezentatívnou povrchovou úpravou. Zábrany, ktoré určujú pohyb osôb, sú vybavené funkciou PANIC.

Rampy a brány: Riadený vstup na parkovisko v rámci objektu je podriadený bezpečnostnému systému s použitím prístupových čítačiek kariet. Prechod motorových vozidiel cez rampy je usmernený signalizačným zariadením.

Úloha:

- evidovanie príchodu a odchodu pracovníkov v služobných motorových vozidlách a nákladných služobných automobiloch,
- evidovanie príchodu a odchodu návštevných motorových vozidiel,

Riešenie: systém s bezkontaktnými čipovými kartami použitými v bezpečnostnom systéme.

5.4 Režimové opatrenia objektu

- osoby a vozidlá vchádzajú do objektu cez vrátnicu, kde vykonáva kontrolu príslušník strážnej služby,
- zamestnanci sa preukazujú preukazom vstupu do objektu (čipovú kartu), tento preukaz sú povinní nosiť po celú dobu nachádzania sa v objekte,
- automobily a nákladné autá vstupujúce do objektu musia mať na viditeľnom mieste kartu povolenia vstupu a musia parkovať iba na miestach pre nich určených,
- používanie mobilných telefónov je povolené iba v miestnostiach na to určených, používanie mobilných telefónov, audio a video záznamových zariadení je v priestoroch výrobnej haly zakázané,
- ochranu objektu v čase pracovnej doby a mimo pracovnej doby zaisťuje strážna služba,
- návštevy sa musia legitimovať a ostať v návštevnej miestnosti, po objekte sa môžu pohybovať iba v sprievode poverenej osoby,
- zamestnanci môžu vstupovať iba do priestorov pre nich určených,
- vstup zamestnancom je umožnený bezkontaktnou čipovou kartou zamestnanca, iba do priestorov kde majú vstup povolený, vstupovať do iných priestorov môže iba so súhlasom riaditeľa prevádzky,
- s mechanickými zábrannými prostriedkami akými sú vstupné brány, závory a rampy, môžu manipulovať iba osoby k tomu určené, v našom prípade službukonajúca strážna služba,
- pri pokuse o narušenie objektu alebo pri narušení objektu je strážna služba povinná vykonať opatrenia vyplývajúce zo situácie a v prípade potreby informovať políciu slovenskej republiky alebo iné na to slúžiace orgány, potom informovať riaditeľa podniku alebo zástupcu riaditeľa,
- pri vzniku mimoriadnej udalosti sa postupuje podľa smerníc alebo plánu na ochranu alebo evakuáciu osôb.

5.5 1. modelová situácia

Zmluvný odberateľ komponentov vyžaduje od dodávateľa dodať dva kamióny produktov denne, a to o 10:00 hod a o 16:00 hod. Kamión pristavený k naloženiu o 15:00 hod sa po zacúvaní k nákladnej rampe pokazil. Zlomila sa mu zadná náprava. Vytiahnutie nie je

možné v krátkej dobe. Z dôvodu neporušenia zmluvných dodávok, musí riaditeľ rýchlo jednať a vyriešiť danú situáciu.

5.5.1 1. aktívne režimové opatrenie

Riaditeľ má tri možnosti:

- okamžité odtiahnutie nákladného auta aby uvoľnil rampu,
- dohodnúť sa z odberateľom, že mu dodajú komponenty až po oprave a uvoľnení rampy, čo môže trvať niekoľko hodín,
- naložiť komponenty iným spôsobom mimo nákladnej rampy

Na základe situácie rozhodol riaditeľ podniku o vydaní aktívneho režimového opatrenia. Najlepšie riešenie je naložiť komponenty iným spôsob mimo nákladnej rampy. Zamestnanci musia postupovať podľa vydaného režimového opatrenia riaditeľa podniku s nasledujúcim rozsahom:

- zamestnanci budú využívať núdzový východ na vstup a výstup z výrobnej budovy,
- k naloženiu nového kamióna sa využije vchode pre zamestnancov,
- vedúci zmeny zabezpečí voľný priechod pre vysokozdvižné vozíky s paletami zo skladu cez východ pre zamestnancov von,
- vedúci zmeny zabezpečí vo výrobnej hale voľný priechod pre vysokozdvižné vozíky v šírke tri metre,
- tento priestor označiť páskou, aby tam nevstupovali iné osoby,
- ku vchodu je potrebné pristaviť kamión a vytvoriť voľný priestor okolo neho potrebný k nakladaniu tovaru,
- priestor okolo kamióna sa ohradí rozlišovacou páskou,
- vysokozdvižné vozíky sa budú pohybovať po jednom, vždy jeden bude nakladať tovar a druhý v tom istom čase vykladať do kamióna,
- vedúci zmeny poverí osoby, ktoré budú dohliadať na priechodnosť trasy vysokozdvižných vozíkov,
- tieto osoby budú rozlíšené výstražnými vestami,
- po naložení materiálu vedúci zmeny bude zodpovedať za znovuobnovenie činnosti prevádzky a uvedenie vecí do normálneho stavu,
- vedúci zmeny podá riaditeľovi o ukončení akcie informáciu.

5.6 2. modelová situácia

Prístupová cesta k vrátnici je z dôvodu náhlej rekonštrukcie uzavretá. Aby sa nezastavila výroba v podniku je nutné aby riaditeľ vydal aktívne opatrenia na vyriešenie vstupu zamestnancov a vjazdu automobilov.

5.6.1 2. aktívne režimové opatrenie

Riaditeľ podniku musí vydať aktívne režimové opatrenie o využití zadnej brány pre vstup osôb a vjazd automobilov.

Postup je nasledovný:

- hlavný vchod do podniku sa uzavrie,
- strážna služba konajúca službu na vrátnici sa presunie k zadnej bráne,
- 1 strážnik zostane na vrátnici pri hlavnom vstupe,
- zabezpečí sa spojenie medzi hlavným a zadným vchodom do objektu, v prípade zlyhania linky budú strážnici opatrení vysielačkami,
- vedúci strážnik poverí osobu, ktorá odkloní dopravu k zadnému vchodu,
- službu konajúci strážnik bude opatrený výstražnou vestou a pri zadnom vchode bude vykonávať kontrolu vstupu osôb a vjazdu automobilov,
- o všetkom bude vedúci strážnik informovať riaditeľa.

ZÁVER

Objektová bezpečnosť je aktuálnou témou, ktorá plní nezastupiteľnú úlohu funkcií ochrany majetku a osôb. Ide o veľmi dôležitú a náročnú činnosť, ktorú predchádza veľké množstvo príprav. Je dôležité aby zabezpečenie objektu bolo jednoznačné, účinné a hlavne spoľahlivé. Komplex zabezpečenia ochrany objektov zaistíme nie len kombináciou fyzickej a technickej ochrany ale aj zložkou, ktorá je pri ochrane majetku veľmi dôležitá a zabúdaná, a to režimovými opatreniami podniku. Zaistenie ochrany objektov a areálov je náročný priebeh činností, ktorý sa začína analýzou zraniteľnosti objektu. Ide o kľúčový bod celého postupu ochrany. Ďalšou dôležitou činnosťou je spracovanie bezpečnostného projektu a bezpečnostnej politiky podniku. Nemôžeme však zabúdať ani na legislatívnu podporu, ktorá sa týka zabezpečenia objektov.

Zlepšenie zaistenia ochrany objektov a budov zaistíme integráciou bezpečnostných systémov, čím dosiahneme úplné komfortné a hlavne spoľahlivé zaistenie ochrany nášho majetku. Inteligentné budovy predstavujú systém luxusného riadenia funkcii celej budovy akými sú kúrenie, osvetlenie, vetranie, otváranie dverí, otváranie roliet a iných činností, ktoré súvisia, aj keď to tak nevyzerá, s činnosťou bezpečnostných systémov. Umožňujú napríklad systém naprogramovať tak, aby v prípade indikovania vniknutia neoprávnenej osoby do objektu zažal svetlá alebo zamkol dvere k iným častiam domu, či iné činnosti, ktoré znepríjemnia narušiteľovi čas strávený v objekte.

V mojej bakalárskej práci som sa snažila popísať správne zaistenie objektovej bezpečnosti a navrhnúť účinné vzorové režimové opatrenia pre priemyselné areály. Táto tematika je veľmi rozsiahla a vyžaduje si dlhodobý proces príprav a činností avšak pokiaľ zaistenie ochrany vykonáme správne, vložené úsilie sa nám vráti späť v podobe bezpečia. Preto budem rada ak táto práca bude aspoň minimálnym prínosom pre jej čitateľov a pomôže im vyriešiť otázky, ktoré sa týkajú témy objektovej bezpečnosti a režimových opatrení.

ZÁVER V ANGLIČTINE

Building security is a current issue, which features an irreplaceable role in protecting property and persons. This is a very important and demanding activity, which needs a large amount of preparations. It is important that ensure of the building was clear, effective and mostly reliable. Complex to ensure the protection of buildings we provide not only a combination of physical and technical protection but also with component of which is very important in protecting of property and is forgetting. This component is regime measures of company. Ensure the protection of buildings and sites is a challenging course of action, which starts with an analysis of vulnerability of the object. It is a main point of the whole procedure. Another important activity is the processing of security projects and security policy of company. We cannot forget the legislative support relating to security objects.

Improvement to ensure the protection of objects and buildings we will ensure the integration of security systems, so we can achieve full, comfort and especially reliable protection of our property. Intelligent buildings represent a system of luxury management of functions throughout the building such as heating, lighting, ventilation, open doors, blinds and other activity related with the operation of safety system, although it does not look so. For example, they allow to program the system so that if case of finding intrusion by unauthorized person or object, to sparked lights or to locked the door to other parts of the house, or other activities that will unpleasant the time spended in the house for violator.

In this bachelor thesis I tried to describe correct ensure of security of building and propose effective, specimen regime measures for industrial facilities. This topic is very extensive and requires a long process of preparation and activities but if we will perform ensure of protection correctly, our effort will be recovered back in the form of security. Therefore I will be glad if this work will be at least the minimum benefit for its readers and will help them to resolve issues related to security of building and regime measures.

ZOZNAM POUŽITEJ LITERATÚRY

[1] KAMENÍK, Jiří; BRABEC, František. Komerční bezpečnost: Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. vyd.1. Praha 3 : ASPI, 2007. 338 s. ISBN 978-80-7357-309-6.

[2] Národný bezpečnostný úrad [online]. 2010 [cit. 2011-02-15]. Národný bezpečnostný úrad. Dostupné z WWW: <http://www.nbusr.sk/sk/index.html>.

[3] LAUCKÝ, Vladimír. Technologie Komerční bezpečnosti II. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. 123 s. ISBN 978-80-7318-631-9.

[4] LOVEČEK, Tomáš ; VEĽAS, Andrej . Zásady a princípy anlýzy rizík v oblasti fyzickej a objektovej bezpečnosti. In Hofreiter, Ladislav . Zásady a princípy anlýzy rizík v oblasti fyzickej a objektovej bezpečnosti [online]. [s.l.] : [s.n.], 2006 [cit. 2011-03-20]. Dostupné z WWW: <www.nbusr.sk>.

[5] FOJTÍK, Daniel . Systémy kontroly vstupu pro kombinované a integrované systémy [online]. [s.l.], 2010. 88 s. Diplomová práce. Univerzita Tomáše Bati ve Zlíne. Dostupné z WWW: <https://portal.utb.cz/wps/PA_StagPortletsJSR168/KvalifPraceDownloadServlet?typ=1&adipidno=16277>.

[6] BRABEC, František. Ochrana bezpečnosti podniku. [s.l.] : [s.n.], 1996. 203 s. ISBN 80-85858-29-0.

[7] UHLÁŘ, Jan. TECHNICKÁ OCHRANA OBJEKTŮ II. DÍL : ELEKTRICKÉ ZABEZPEČOVACÍ SYSTÉMY II. PRAHA : [s.n.], 2009. 229 s. ISBN 978-80-7251-313-0.

[8] ČANDÍK, Marek. Objektová bezpečnost II. Zlín : [s.n.], 2004. 100 s. ISBN 80-7318-217-3.

[9] LAUCKÝ, VLADIMÍR. TECHNOLOGIE KOMERČNÍ BEZPEČNOSTI I. ZLÍN : [s.n.], 2010. 81 s.ISBN 978-80-7318-889-4.

[10] BTSM 2007. SBORNÍK Medzinárodní konference : Bezpečnostní technologie Systémy a Management. Zlín : [s.n.], 2007. 261 s. ISBN 978-80-7318-605-0.

[11] ŠENOVSKY, Michail ; DUDÁČEK, Aleš ; ŠENOVSKÝ, Vít. Ochrana budov zvláštního významu. SECURITY. 2010, 96, s. 48-54.

[12] Antes [online]. 20.5.2005 [cit. 2011-04-23]. Integrovaný bezpečnostný systém. Dostupné z WWW: <http://www.antes.sk/ibs.html>.

[13] KŘEČEK, Stanislav . PŘÍRUČKA ZABEZPEČOVACÍ TECHNIKY. [s.l.] : [s.n.], 2006. 313 s. ISBN 80-902938-2-4.

[14] HURTA, Josef; LAUCKÝ, Vladimír. Management bezpečnostního inženýrství. Zlín : [s.n.], 2006. 172 s. ISBN 80-7318-412-5.

[15] LAUCKÝ, Vladimír. Řízení technologických procesů v průmyslu komerční bezpečnosti. Zlín : [s.n.], 2006. 101 s. ISBN 80-7318-432-X.

[16] UHLÁŘ, Jan. TECHNICKÁ OCHRANA OBJEKTŮ I : MECHANICKÉ ZÁBRANNÉ SYSTÉMY II. Praha : [s.n.], 2009. 179 s. ISBN 978-80-7251-312-2.

[17] LAUCKÝ, Vladimír. SPECIÁLNÍ BEZPEČNOSTNÍ TECHNOLOGIE. Zlín : [s.n.], 2009. 223 s. ISBN 978-80-7318-762-0.

[18] ZÁLEŠÁK, Martin. Technika prostředí v oboru Integrované systémy v budovách. [s.l.] : [s.n.], 2009. 42 s. ISBN 978-80-7318-834-4.

[19] Acsline.cz [online]. 2010 [cit. 2011-05-08]. Acsline. Dostupné z WWW: <www.acsline.cz>.

[20] E-shop.jablotron.sk [online]. 2010 [cit. 2011-05-08]. E-shop.jablotron. Dostupné z WWW: <www.jablotron.sk>.

[21] Slovensko. 215/2004 Zákon o ochrane utajovaných skutočností . In Zbierka zákonov, Slovenská republika. , čiastka 1, s. 1-30.

[22] Česko. 412/2005 Zákon o ochrane utajovaných informácií a o bezpečnostnej spôsobilosti v ČR. In Zbírka zákonů, Česká republika. , částka 1, s. 1- 50.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

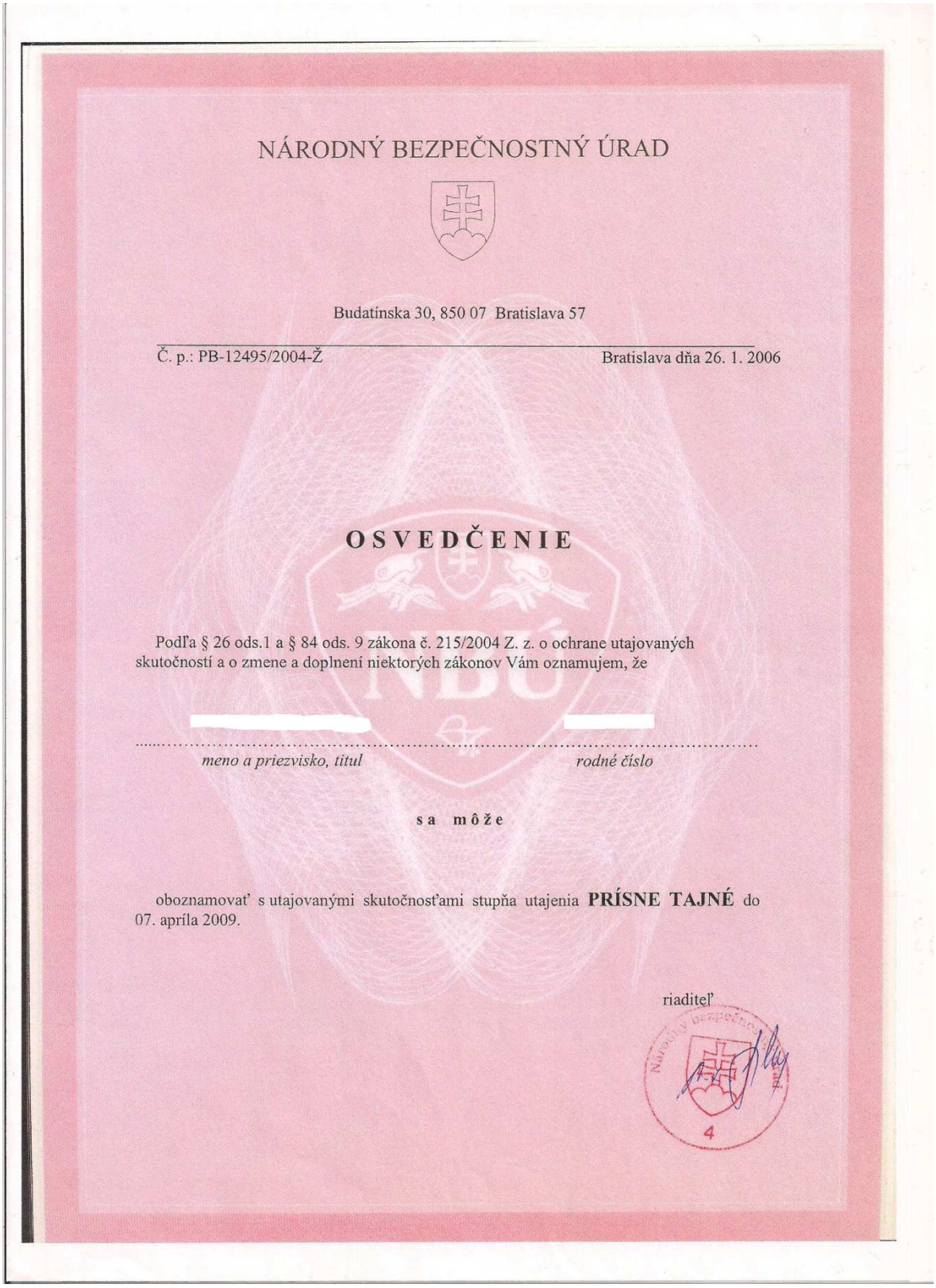
AIR	Activ Infrared – aktívny infračervený detektor.
BD	Bezpečnostná dokumentácia.
CCTV	Closed Circuit Television - uzavretý televízny okruh.
EN	Európska norma.
EPS	Elektrická požiarna signalizácia.
FO	Fyzická ochrana.
LIDAR	Light Detection And Ranging – laserový lokátor.
MZP	Mechanické zábranné prostriedky.
NBÚ	Národný bezpečnostný úrad.
OUS	Ochrana utajovaných skutočností.
PCO	Pult centrálnej ochrany.
PIR	Passive Infrared – pasívny infračervený detektor.
PIRAMID	Pasive InfraRed And Microwave Intruder Detector – duálny pasívny infračervený detektor a mikrovlnný detektor.
PZS	Poplachové zabezpečovacie systémy.
SE	Monitorovacie a signalizačné systém.
SO	Systém organizačných opatrení a fyzickej ochrany.
VKV	Veľmi krátke vlny.

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PŘÍLOHA P I: PREVIERKA



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Budatínska 30, 850 07 Bratislava 57

Č. p.: PB-12495/2004-Ž Bratislava dňa 26. 1. 2006

O S V E D Č E N I E

Podľa § 26 ods.1 a § 84 ods. 9 zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov Vám oznamujem, že

[redacted] [redacted]

meno a priezvisko, titul *rodné číslo*

s a m ô ž e

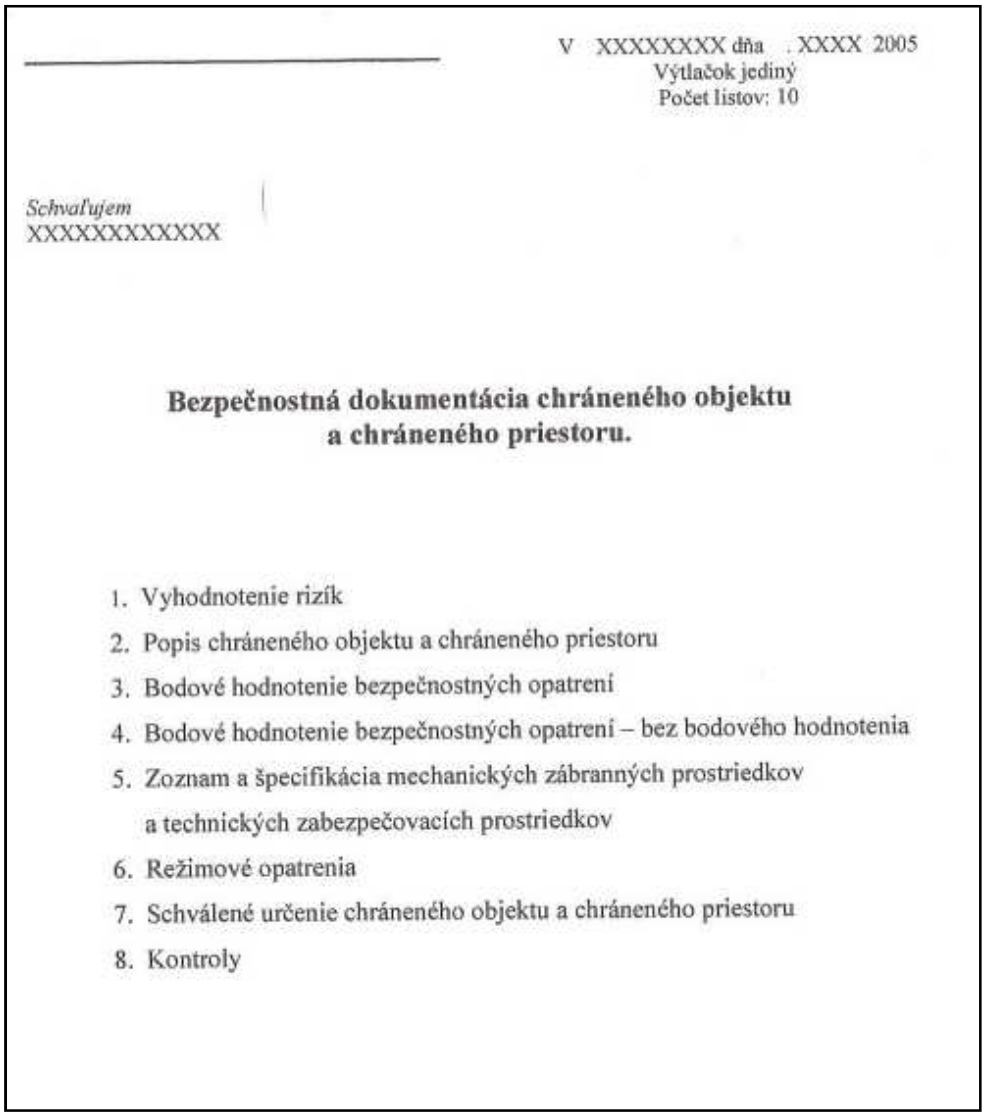
oboznamovať s utajovanými skutočnosťami stupňa utajenia **PRÍSNE TAJNÉ** do 07. apríla 2009.

riaditeľ

4

Príloha 1, Previerka

PŘÍLOHA P II: BEZPEČNOSTNÁ DOKUMNETÁCIA OBJEKTU



V XXXXXXXX dňa . XXXX 2005
Výtlačok jediný
Počet listov: 10

Schvaľujem
XXXXXXXXXXXX

Bezpečnostná dokumentácia chráneného objektu a chráneného priestoru.

1. Vyhodnotenie rizík
2. Popis chráneného objektu a chráneného priestoru
3. Bodové hodnotenie bezpečnostných opatrení
4. Bodové hodnotenie bezpečnostných opatrení – bez bodového hodnotenia
5. Zoznam a špecifikácia mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov
6. Režimové opatrenia
7. Schválené určenie chráneného objektu a chráneného priestoru
8. Kontroly

Príloha 2 Bezpečnostná dokumentácia chráneného objektu

1. VYHODNOTENIE RIZÍK

a) V chránenom priestore sú spracovávané a uchovávané len utajované skutočnosti stupňa utajenia VYHRADENÉ.

b) počet spracovávaných a uchovávaných utajovaných písomností je minimálny.

c) do chráneného priestoru majú prístup len oprávnené osoby určené vedúcim:

- z. XXXXXXXX
- z. XXXXXXXX
- z. XXXXXXXX
- z. XXXXXXXX
- z. XXXXXXXX
- z. XXXXXXXX
- z. XXXXXXXX
- z. XXXXXXXX
- z. XXXXXXXX

d) Okrem určených zamestnancov nemá nik iný prístup do chráneného priestoru.

e) Riziká ohrozenia utajovaných skutočností sú minimálne. Chránený priestor na nachádza na 2 nadzemnom podlaží. Vstup na 2. nadzemné podlažie je chránený oceľovou vstupnou mrežou vybavenou visiacim zámkom triedy odolnosti I. Od tejto mreže majú kľúče len oprávnené osoby. Vstupné dvere do chráneného priestoru sú vybavené bezpečnostný zámkom triedy odolnosti I a počas nepritomnosti zamestnancov aj zapečatené. Okolité budovy nepredstavujú pre chránený priestor nijaké riziko.

Kľúče od chráneného priestoru má právo vyzdvihnúť len:

- z. XXXXXXXXX
- z. XXXXXXXX
- z. XXXXXXX

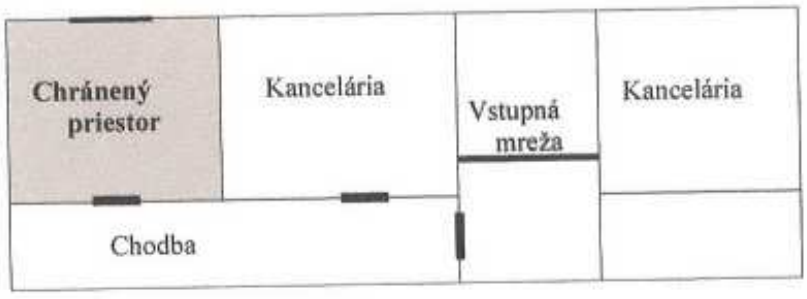
f) Riziko ohrozenia utajovaných skutočnosti v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu sú vzhľadom na malý počet uchovávaných utajovaných skutočností minimálny.

a) Chránený objekt je zároveň aj chránený priestor.

b) Adresa chráneného priestoru je: XXXXXXXXX

c) Chránený priestor tvorí jedna miestnosť. Vstup do miestnosti je cez jedny vstupné dvere. Steny chráneného priestoru sú vymurované z tehál a hrúbky 55 cm. V chránenom priestore je jedno okno o rozmeroch 240 x 200 cm a je umiestnené 6 m nad okolitým terénom.

d) Nákres hraníc chráneného objektu a priestoru.



Chránený priestor Posádkovej správy budov Nové Mesto nad Váhom.
Kategória VYHRADENÉ.
Chránený priestor slúži na spracovávanie a ukladanie utajovaných písomností.

BEZPECNOSTNÉ OPATRENIE	TYP	BODOVÉ OHODNOTENIE
Úschovné objekty (bod 1.1.)	T.4 – 4body T.3 – 3body T.2 – 2body T.1 – 1 bod	SS1 = 2
Zámky úschovných objektov (bod 1.2.)	T.4 – 4body T.3 – 3body T.2 – 2body T.1 – 1 bod	SS2 = 2
Celkové ohodnotenie úschovného objektu a jeho zámku (bod 11.1.)	S1 = SS1 x SS2	**S1 = 4**
Chránený priestor (bod 2.1.)	T.4 – 4body T.3 – 3body T.2 – 2body T.1 – 1 bod	SS3 = 1
Uzamykacie systémy určené na uzamykanie chránených priestorov (bod 2.2.)	T.4 – 4body T.3 – 3body T.2 – 2body T.1 – 1 bod	SS4 = 1
Celkové ohodnotenie ochrany chráneného priestoru (bod 11.2.)	S2 = SS3 + SS4	**S2 = 3**
Objekt (bod 3.)		**S3 = 0**
Povinné (S1) + (S2) + (S3)	(S1) + (S2) + (S3)	**7**
Kontrola vstupu (bod 4.1.)	T.4 – 4body T.3 – 3body T.2 – 2body T.1 – 1 bod	SS6 = 1
Režim návštev v objekte (bod 4.3.) a) Návštevy sprevádzané b) Návštevy nesprevádzané	ad a) – 1 bod ad b) – 0 bodov	SS7 = 1
Celkové ohodnotenie kontroly vstupov a režimu návštev (bod 11.4.)	S4 = SS6 + SS7	**S4 = 2**
Fyzická ochrana (bod 5.1.)	T.5 –5bodov T.4 – 4body T.3 – 3body T.2 – 2body T.1 – 1 bod	SS8 = 1
Technická úroveň prostriedkov EZS (bod 5.2.1.)	T.4 – 4body T.3 – 3body T.2 – 2body T.1 – 1 bod	SS91 = 0