BEZPEČNOSTNÉ EXPERTÍZY OBJEKTOV V SLOVENSKEJ REPUBLIKE AKO HLAVNÝ NÁSTROJ TAKTIKY A TECHNIKY V PKB

Security expertise of objects in the Slovak Republic as the main tool of tactics and techniques in PKB

Bc. Zuzana Svrbíková

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Zuzana SVRBÍKOVÁ**
Osobní číslo:	**A09459**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnostní expertízy objektů ve Slovenské republice jako hlavní nástroj taktiky a techniky v Průmyslu komerční bezpečnosti**

Zásady pro vypracování:

Cíl: Vypracovat pracovní manuál pro managery PKB pro výkon bezpečnostní expertízy objektů.

1. **Úvod, východiska a hledání správneho postupu zpracování bezpečnostní expertízy v dnešní praxi.**
2. **Taktika zprac. bezp. anylýzy a prognózy, bezp. plánování a bezpečnostní projekt a jejich realizace.**
3. **Syntéza problému a možné chybné postupy.**
4. **Praktická ukázka bezp. expertízy v reálnem objektě. 5. Technické zajištení problematiky s využitím IT.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Brabec, František, vedoucí autorského kolektívu, Bezpečnosť pro firmu, úřad, občana**
2. **Laucký, Vladimír, Judr., Technologie komerční bezpečnosti I**
3. **Laucký, Vladimír, Judr., Technologie komerční bezpečnosti II**
4. **Laucký, Vladimír, JUDr., Řízení technologických procesú v průmyslu komerční bezpečnosti**
5. **Zákon Slovenskej republiky č 215/2004 Z.z o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov**
6. **Vyhláška Národného bezpečnostného úradu 331/2004 o personálnej bezpečnosti a o skúške bezpečnostného zamestnanca**
7. **Zákon Slovenskej republiky č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov**
8. **Fico, Róbert, Nutná obrana**

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

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

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cieľom mojej diplomovej práce bolo spracovať bezpečnostný projekt na konkrétnom objekte v Slovenskej republike a predložiť manažérsky manuál pri vykonávaní objektových expertíz, ktorého dôležitou súčasťou je kvalitne spracovaný systém ochrany súkromných bezpečnostných služieb.

Klíčová slova: bezpečnostná expertíza, analýza, bezpečnostný projekt, súkromná bezpečnostná služba, objektová bezpečnosť, personálna bezpečnosť, bezpečnosť informačných technológií.

ABSTRACT

The aim of my dissertation was to develop a security project on a particular house in the Slovak republic and present management manual by implementing of expertise in the object, the important component is in a high quality made system of protection of private security services.

Keywords: security expertise, analysis, security project, private security service, object security, personnel security, information technology security.

Týmto ďakujem svojmu vedúcemu diplomovej práce JUDr. Vladimírovi Lauckému za odborné a svedomité vedenie pri spracovaní tejto témy.

Ďalej by som chcela poďakovať Jánovi Svrbíkovi za odborné konzultácie k danej téme a Ing. Ivanovi Šupákovi, koordinátorovi bezpečnosti, za podporu a umožnenie spracovania bezpečnostného projektu firmy IMV Industry s.r.o.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/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 diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/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 diplomovou/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 – diplomovou/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 diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

1. ÚVOD

Problematiku spojenú s ochranou a bezpečnosťou sa snažia ľudia vyriešiť už počiatku vekov. Zabezpečenie majetku a ochrana zdravia a života boli mnohoraké , no postupne sa vykryštalizovali tri veľké skupiny:

a.) Všetko, čo je spojené so samotnou podstatou fyzickej existencie ľudí = ZDRAVIE A ŽIVOT

b.) Všetko, čo je spojené s vlastníckymi vzťahmi k hmotným veciam a k majetkovým právam (nehmotným veciam), = MATERIÁLNA EXISTENCIA

c.) Všetko, čo je spojené s presadzovaním a ochranou záujmov jednotlivých osôb (fyzických i právnických), = SKUPINOVÁ EXISTENCIA

Medzi týmito tromi skupinami objektov neexistuje nepreniknuteľná priehrada, pretože často narušenie ktoréhokoľvek z nich môže viesť k narušeniu ostatných dvoch. Nakoľko následok môže mať radu príčin, tak i príčina môže vyvolať radu následkov.

Prostriedky, ktoré ľudstvo k zaisteniu svojej bezpečnosti používa, sa postupom stáročí mení, i keď niektoré zostávajú vo svojej podstate rovnaké – len zmodernizované prostredníctvom nových technológií.

Aj to, čo kedysi spoľahlivo plnilo svoju funkciu, napr. vodná priekopa okolo stredovekého hradu, po čase túto schopnosť stráca. Je to prirodzený proces , ktorý súvisí nie len s rozvojom stále modernejších technológií, ale často i s prekonávaním psychologických bariér, konvencií a stereotypov ľudských činností.

Aj naša doba sa zaradí do histórie a i my prispejeme svojim dielom k tejto nekonečnej rade príkladov, ako sa ľudia snažia dosiahnuť dokonalej a trvalej bezpečnosti pred možným narušením a útokom. Tento fakt „obmedzenosti“ a „pominuteľnosti“ však neznižuje ľudskú snahu dosiahnuť dokonalého spôsobu zaistenia bezpečnosti našich troch veľkých skupín objektov.

Na základe našich zistených skutočností nám umožňuje definovať:

- Cieľ zabezpečenia (v zmysle dosiahnutia určitého definovaného stavu – istoty)

- Objekt zabezpečenia (tj. Život alebo zdravie fyzickej osoby, vlastnícke a obdobné práva osôb, organizácií, inštitúcií a štátu a záujmov jednotlivcov, organizácií, inštitúcií a štátu)
- Spôsob a prostriedky zabezpečenia
- Materiálové a finančné náklady na vykonanie zabezpečenia
- Termíny, do kedy je zabezpečenie nutné realizovať
- Osoby, ktoré za vykonanie zabezpečenia nesú osobnú zodpovednosť.

Určitá úroveň poznania nám umožní nájsť správne odpovede na uvedené otázky. Určí nám minimálne podmienky, ktoré musíme splniť, aby sme docielili požadovanú mieru istoty. Úroveň, účinnosť, použité prostriedky a náklady na zabezpečenie sú priamou reflexiou miery zabezpečenia alebo ohrozenia.

V procese vedúcom k dosiahnutiu požadovaného stavu je potrebná úroveň znalostí výsledkom zberu údajov, informácií a dát o zabezpečovanom objekte a ich analýzy. Pretože predmetom tejto analýzy sú skutočnosti týkajúce sa zabezpečenia príslušného objektu a výsledkom tejto analýzy má byť zistenie stávajúceho stavu zabezpečenia, ide o bezpečnostnú analýzu.

Bezpečnostná analýza je východiskom pre proces syntézy získaných poznatkov a vypracovania bezpečnostného projektu, ktorého úlohou je určiť konkrétne opatrenia, ktorými bude dosiahnutý cieľ definovaný bezpečnostnou politikou. Pritom bezpečnosť nemožno chápať ako prostý súhrn použitých prostriedkov, opatrení a postupov, ale ako celok – systém, ktorý je vytvorený za účelom dosiahnutia konkrétneho cieľu.

Aby tento systém fungoval, musí byť schopný reagovať na zmeny vonkajších podmienok tak, aby sa im operatívne prispôsobil, bez toho, aby bolo znížená jeho funkčnosť. Musí však byť schopný reagovať nie len na zmeny, ktoré už prebehli alebo práve prebiehajú, ale aj na zmeny, ktoré majú alebo môžu nastať v budúcnosti.

Výsledkom takej analýzy je okrem zistenia súčasného stavu veci aj zistenie predpokladaného budúceho vývoja formulovaného v podobe bezpečnostnej prognózy. Schopnosť prognózovať presne a konzistentne je veľmi dôležitá, avšak úplná presnosť je nedosiahnuteľná.

Zásadné informácie pre bezpečnostnú expertízu organizácie nie sú v podobe presných čísiel, čo samozrejme obmedzuje možnosti výberu a použitia rôznych techník analýzy

a prognózy. Dá sa povedať, že každá odborná poradenská organizácia v oblasti zabezpečenia si vypracovala vlastné postupy, ktoré sú modifikáciou bežne používaných techník strategickej analýzy v iných oblastiach.

K vykonaniu bezpečnostnej analýzy môžeme použiť mnoho techník a rôzne prístupy k vyhodnoteniu získaných informácií a dát, no jednu dôležitú zložku ako je analýza rizík nemôžeme vynechať. Bez vykonania tejto analýzy by bezpečnostná analýza nebola kompletná, ani použiteľná pre funkčné riešenie problému bezpečnosti.

Analýza rizík musí dať odpoveď na tri základné otázky:

1. Aké riziká – hrozby môžu nastať,
2. Aká je pravdepodobnosť, že riziká nastanú a dôjde k bezpečnostnému konfliktu,
3. Aké budú následky, keď bezpečnostný konflikt nastane.

Odpovede na tieto otázky nám pomôžu definovať, aké opatrenia majú byť použité, aby bolo dosiahnuté požadovaného cieľa.

Zabezpečenie organizácie tvorí systém opatrení, ktorých cieľom je, aby organizácia ako celok i jej jednotlivé organizačné zložky a jej zamestnanci boli chránený pred vonkajšími i vnútornými vplyvmi .

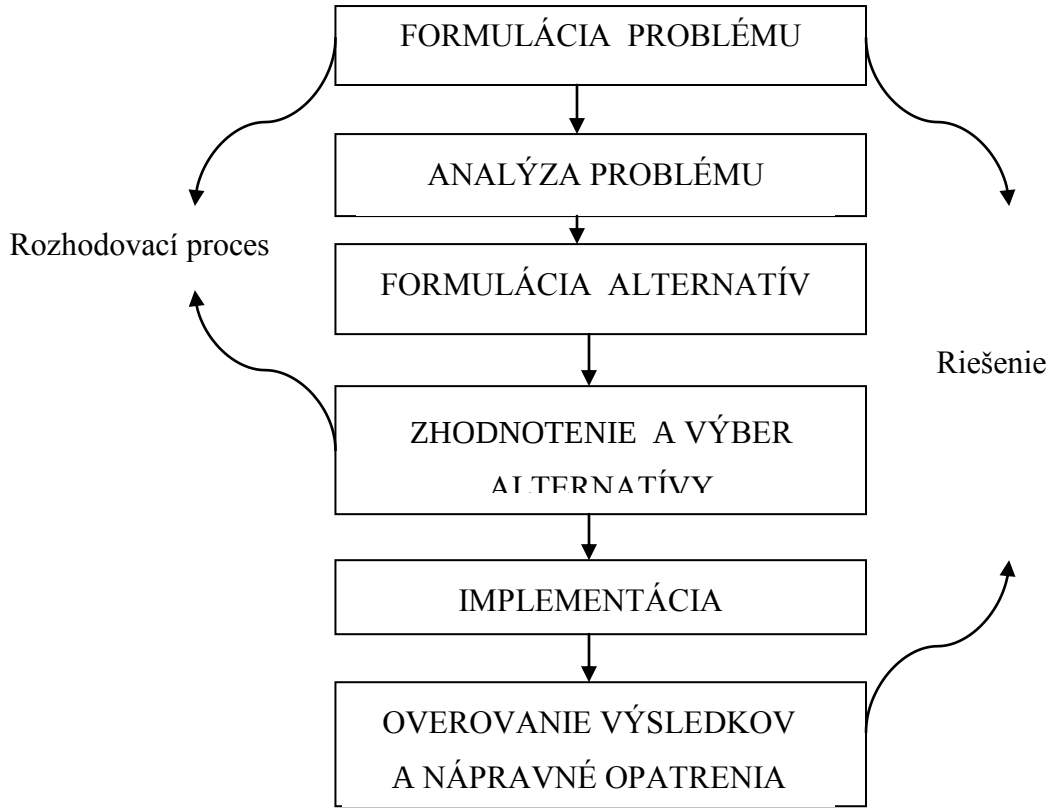
[1]

I. TEORETICKÁ ČASŤ

1 VÝCHODISKÁ PRE SPRACOVANIE BEZPEČNOSTNEJ EXPERTÍZY

Každý, kto rieši problém bezpečnosti organizácie, musí vykonať rad krokov, ktoré sú dané a aj ich poradie je určené. Na počiatku je nevyhnutné problém formulovať. Ak už máme problém formulovaný, je nutné ho analyzovať. Výsledkom analýzy bude určenie možností riešenia problému, presnejšie formulovať alternatívy riešenia. Fáza, ktorá nasleduje, je veľmi dôležitá, pretože v nej dochádza k posúdeniu jednotlivých alternatív riešenia a k výberu jednej z alternatív. Ďalším krokom k vyriešeniu problému je implementácia rozhodnutia. Proces riešenia problému by mal tiež vždy obsahovať spätnú väzbu – overovanie výsledkov rozhodnutia a prijatie nápravných opatrení.

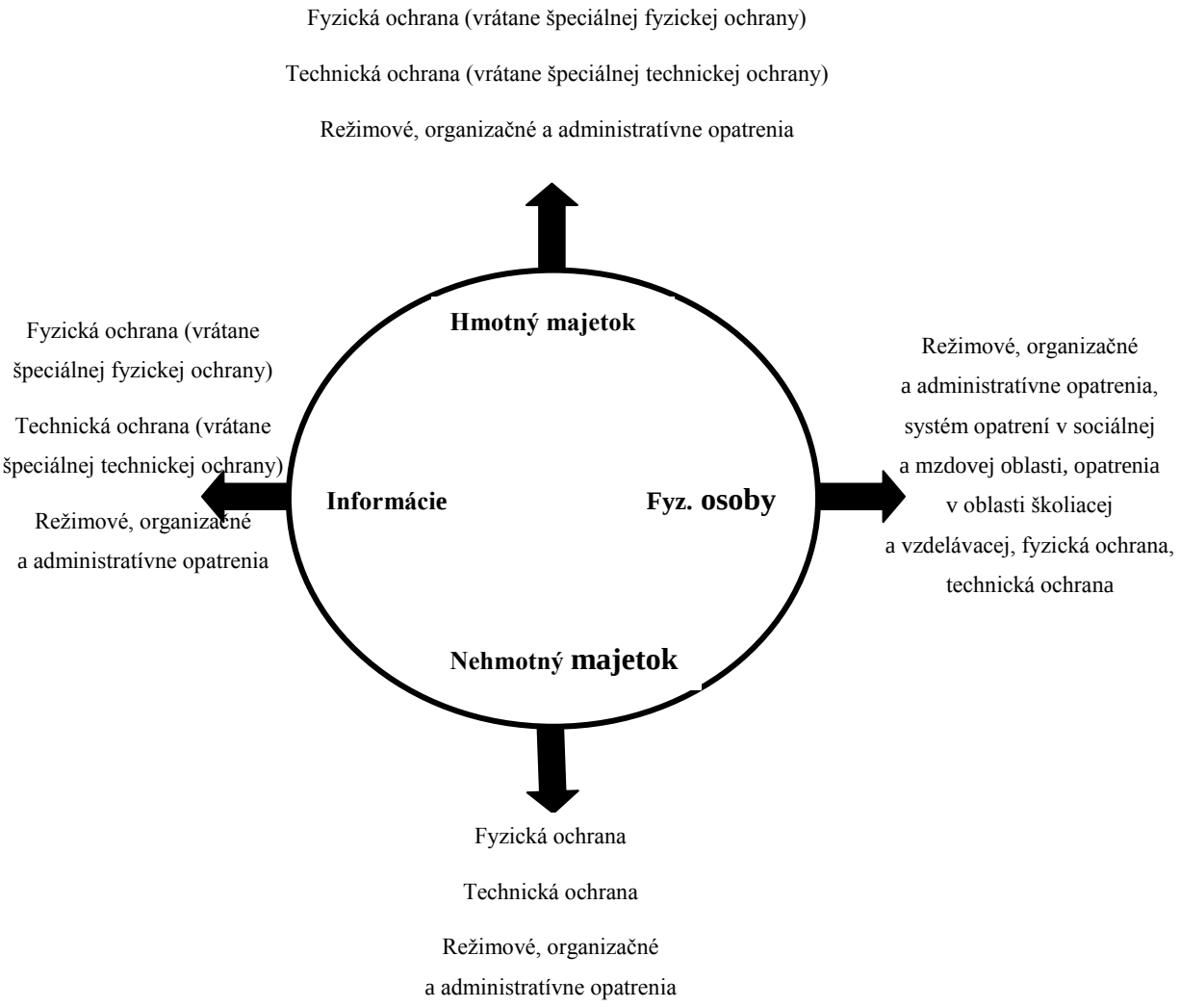
Grafické zobrazenie:



V oblasti zabezpečenia sa formulácie „problému“ stotožňuje s odpoveďou na otázku : aký stupeň účinnosti zabezpečenia je pre organizáciu potrebný? Odpoveď na túto otázku je veľmi dôležitá, pretože výrazne ovplyvní alebo aj určí, ako bude bezpečnostná expertíza

ďalej prebiehať a aký bude mať rozsah, aké prostriedky a opatrenia budú použité pri realizácii bezpečnostného projektu a aj aké náklady budú musieť byť na expertízu a na realizáciu vynaložené.

Ak teda budeme hovoriť o bezpečnostnej expertíze, máme na mysli komplexnú bezpečnostnú expertízu celej organizácie. Pre postupy a techniky pri vlastnom vykonávaní analýzy nie je rozhodujúce, či sa vykonáva komplexná bezpečnostná expertíza celej organizácie alebo len čiastočná bezpečnostná expertíza. Rozdiely medzi komplexnou a čiastočnou bezpečnostnou expertízou organizácie nachádzame len v šírke skúmaných skutočností, v miere prácnosti a v počte a v zložitosti skúmaných vzájomných väzieb a súvislostí.



Komplexná bezpečnostná expertíza organizácie skúma spôsob, rozsah a úroveň zabezpečenia jednotlivých objektov ochrany v organizácii. Objekty, ktoré je nutné v organizácii chrániť je možné rozdeliť do troch skupín:

1. Majetok (hmotný a nehmotný)
2. Fyzické osoby (resp. ich život a zdravie)
3. Informácie (ochrana oprávnených záujmov organizácie)

Veľmi dôležité je pochopiť, že organizácia nechráni len tie objekty, ktoré sú súčasťou jej samotnej (vlastný majetok, vlastní zamestnanci a vlastné informácie), ale tiež objekty, ktoré sú mimo nej (cudzí majetok, iné fyzické osoby, iné informácie a záujmy iných subjektov).

K dosiahnutiu potrebného stupňa zabezpečenia sa potom v praxi používajú tieto štyri základné skupiny bezpečnostných opatrení a prostriedkov:

1. Fyzická ochrana
2. Technická ochrana
3. Administratívne organizačné a režimové opatrenia
4. Kombinácia predchádzajúcich prostriedkov a opatrení

Medzi najzákladnejšie obecné faktory, ktoré ovplyvňujú výber vhodného prostriedku či opatrenia, je miera rizika, ktorá objektu ochrany hrozí.

[1]

2 PRÍSTUP KU SPRACOVANIU BEZPEČNOSTNEJ EXPERTÍZY

U komplexnej bezpečnostnej analýzy organizácie, ktorá je v prípade komplexnej bezpečnostnej expertízy nevyhnutná, je predmetom analýzy bezpečnosť organizácie ako celok. Analyzovať sa musia všetky vnútorné i vonkajšie záležitosti, ktoré ovplyvňujú bezpečný chod organizácie.

Základom vykonania analýzy je však správna formulácia problému, čo dosiahneme zberom a triedením informácií. Musí sa hlavne jednať o informácie, ktoré relevantne ovplyvňujú formulovanie problému a vytýčenie cieľa. Nepodstatné informácie len zaťažujú analytikov, zvyšujú prácnosť, predlžujú termín dokončenia, zvyšujú náklady a prispievajú k chybným záverom. Relevantnosť informácie musí byť zrejmá už od počiatku. Až v priebehu prác sa môže objaviť pravý význam informácie, ktorá bola predtým zamietnutá.

Príklad: Pre zabezpečenie miestnosti, v ktorej je umiestnená pokladňa podniku a kde sa počítajú mzdy, je relevantná informácia napr. architektonické a stavebné riešenie miestnosti, počet okien a dverí, či sú použité mechanické bezpečnostné prostriedky (mreže, bezpečnostné dvere a pod.), či sú použité elektrické a elektronické prostriedky zabezpečenia (EZS, kamerový systém a pod.), výška dolnej časti rámu okna od vonkajšieho terénu, vzdialenosť okna od ďalších okien alebo balkónov na budove, príp. od iných objektov, možná maximálna výška hotovosti nachádzajúca sa v miestnosti, či sa hotovosť v miestnosti ponecháva cez noc alebo i niekoľko dní alebo v pracovnej dobe, kto má do miestnosti prístup atď. Informácie, ktoré pre daný problém nie sú relevantné, napr. obchodná politika a obchodné záujmy organizácie, administratívne a režimové opatrenia k ochrane skladu výrobkov a pod.

Informácie relevantné pre bezpečnostnú analýzu sú obsiahnuté vnútri organizácie, a to hlavne:

- V základných ustanovujúcich dokumentoch organizácie
- V predmete jej činnosti
- V organizačných a interných predpisoch organizácie, vrátane jej organizačnej štruktúry

- V postavení organizácie v rámci väčšieho organizačného usporiadania (napr. v rámci holdingu apod.)
- V architektonickom a stavebnom riešení objektov, v ktorých organizácia vyvíja svoju činnosť (nie len činnosť, ktorá je predmetom podnikania)
- V personálnom zložení organizácie a zásadách personálnej politiky
- V obchodnej politike organizácie a v ich vytýčených cieľoch
- Vo vnútornej situácii organizácie a jej trendu

Mnoho podstatných informácií môžeme získať i vo vnútri organizácie, a to hlavne:

- V medzinárodných zmluvách a záväzkoch
- V medzinárodných štandardoch a odporučeniach
- V tuzemských štandardoch a odporučeniach
- V interných rezortných predpisoch
- V celospoločenskej situácii a jej trendu

Zdrojom potrebných informácií je v prvom rade samotná organizácia. Veď predsa analyzujeme túto organizáciu, resp. určité jej činnosti a aktivity. Jej písomnosti a dokumenty vypovedajú o skutočnom stave organizácie, o tom, či je problém riešený alebo nie je a aká je kvalita a účinnosť momentálneho riešenia. Zdrojom informácií sú tiež riadiaci a ostatní pracovníci organizácie.

Informácie majú spravidla ustálenú formalizovanú podobu:

- Originálne písomnosti a dokumenty (napr. obecné predpisy, interné predpisy, zmluvy apod.)
- Štatistické výkazy a ročné správy štátnych orgánov a inštitúcií
- Ústne a písomné vyjadrenia a komentáre fyzických osôb k analyzovanému problému
- Dotazníkový prieskum u vybraných pracovníkov organizácie
- Vlastné pozorovanie pracovníkov, ktorí zber informácií vykonávajú
- Informácie získané zo siete Internet apod.

Pretože proces analýzy je v podstate procesom od abstraktného ku konkrétnemu, musí aj triedenie informácií odpovedať tomuto postupu. Informácie triedime v ďalších etapách podľa miery jej abstraktnosti alebo konkrétnosti vo vzťahu k riešenému problému. Informácie môžeme triediť aj podľa časového významu informácie, tzn. či informácia je

významná len pre posúdenie stávajúceho stavu – prítomnosti, alebo je významná i pre budúci vývoj – budúcnosť.

Informácie môžeme rozlíšiť:

Podľa významu

- Ktoré majú vplyv na výsledok analýzy
- Ktoré majú len obmedzený vplyv na riešenie

Podľa dostupnosti

- Verejné (určené pre určitý okruh osôb)
- utajované (určené len pre vybraný okruh pracovníkov).

Podľa vierohodnosti

- vierohodné
- nevierohodné

Podľa oblastí

- personálne
- technické
- administratívne
- organizačné.

Okrem zberu a triedenia informácií vykonávame i zlučovanie informácií do nových celkov. Tento proces nám môže pomôcť v kompletizácii neúplných informácií alebo pri zvýšení kvality informácie jej spresnením. Konečnej analýze podrobíme takto „skompletizovanú“ novú informáciu.

[1]

3 BEZPEČNOSTNÁ ANALÝZA

Bezpečnostná analýza je metóda skúmania, pri ktorej sa vykonáva dekompozícia objektu na základné prvky, vyhľadáva sa a skúma vnútorná zraniteľnosť, vonkajšie hrozby a implementované ochranné mechanizmy, pôsobiace na jednotlivé prvky vo zvolených vrstvách bezpečnosti:

- Personálne
- Administratívne
- Organizačné
- Počítačové
- Komunikačné
- Fyzické
- Technické

Cieľom bezpečnostnej analýzy je identifikovať maximum zraniteľností a nedostatkov obsiahnutých v skúmanom objekte, odhadnúť hrozby, riziká a možné negatívne dopady, určiť efektivitu a funkčnosť stávajúcich ochranných mechanizmov a navrhnúť nové tak, aby boli všetky riziká efektívne znížené alebo pokryté na akceptovateľnú úroveň.

Po preskúmaní predmetov, javov, skutočností a informácií dotýkajúcich sa bezpečnostného systému zákazníka, využitím metód z oblasti krízového manažmentu sa zisťuje aká je pravdepodobnosť, že mimoriadna udalosť nastane, aké budú jej účinky, dopad a vzájomná previazanosť rizík.

<table>
<tr><th colspan="5">Riešenie bezpečnosti</th></tr>
<tr><td colspan="2">Hrozby</td><td rowspan="4">Objekt, organizácia</td><td colspan="2">Protiopatrenia</td></tr>
<tr><td>poruchy</td><td>Prírodná kalamita</td><td>Bezpečnosť IS</td><td>Organizačné opatrenia</td></tr>
<tr><td>Internet</td><td>Požiar</td><td>Bezpečnosť práce</td><td>Požiarna ochrana</td></tr>
<tr><td>Epidémia</td><td>Priemyslová</td><td>Riadenie rizík</td><td>Personálna</td></tr>
</table>

	špionáž			politika
Konkurencia	Úrazy		Audity	Školenia
Zamestnanci	Zlyhanie IS		Politika	Poistenie
Legislatíva	Zásobovanie			Fyzická bezpečnosť
Terorizmus	Kriminalita			

Tabulka č.1 Riešenie bezpečnosti

Niekedy je veľmi dôležité uvedomiť si aký rozdiel je medzi jednotlivými pojmami, ktoré sú pre nás smerodajné pre dôkladné vykonanie bezpečnostnej analýzy.

Hrozba

Pod pojmom hrozba sa skrýva sila, aktivita alebo osoba, ktorá môže spôsobiť škodu (napr. požiar, prírodná katastrofa, krádež zariadenia, zisk informácií neoprávnenou osobou).

Hrozba využije zraniteľnosť, prekoná protiopatrenia a pôsobí na aktívum, kde spôsobí škodu.

Hrozba pôsobí jednak priamo na aktívum alebo na protiopatrenie, s cieľom získať prístup k aktívu. Aby mohla hrozba pôsobiť, musí byť aktivovaná, pre čo vyžaduje zdroje (vytvorenie podmienok pre jej pôsobenie).

Protiopatrenie

Je postup, proces, procedúra, technický prostriedok alebo čokoľvek, čo je určené pre zmiernenie pôsobenia hrozby (jej eliminácii), zníženie zraniteľnosti alebo dopadu hrozby. Protiopatrenia sa navrhujú s cieľom zamedziť vzniku škôd alebo s cieľom uľahčiť preklenutie následkov vzniknutej škody.

Protiopatrenie chráni aktíva, deteguje hrozby a zmierňuje alebo úplne zabraňuje pôsobeniu na aktíva. V neposlednom rade protiopatrenie odradzujú ad aktivovania hrozieb.

Riziko

- Pravdepodobnosť, možnosť vzniku straty
- Odchýlenie skutočných a očakávaných výsledkov
- Nebezpečenstvo negatívnej odchýlky od cieľa (tzv. čisté riziko)
- Nebezpečenstvo chybného rozhodnutia

- Možnosť vzniku straty alebo zisku (tzv. špekulatívne riziko)
- Neurčitosť spojená s vývojom hodnoty aktíva (tzv. investičné riziko)
- Možnosť, že špecifická hrozba využije špecifickú zraniteľnosť systému.

Riziko je možnosť, že s určitou pravdepodobnosťou vznikne udalosť, ktorú považujeme z bezpečnostného hľadiska za nežiaduce.

Riziko je vždy odvoditeľné a odvodené z konkrétnej hrozby.

Mieru rizika, teda pravdepodobnosť škodlivých následkov vyplývajúcich z hrozby a zo zraniteľnosti záujmu, je možno posúdiť na základe tzv. analýzy rizík, ktorá vychádza i s posúdenia našej pripravenosti hrozbám čeliť.

[9]

Bezpečnostné riziko je situácia, ktorá nastane v chránenej organizácii a ktorej dôsledkom môže vzniknúť krízová situácia.

Bezpečnostné riziká delíme na:

- Bezprostredné (okamžite viditeľné)
- Následné (ktoré môžu privodiť značné škody)
- Latentné (skryté) nemusíme na ne vôbec prísť

[2]

Aktívum

Je všetko, čo má pre subjekt hodnotu, ktorá môže byť znehodnotená pôsobením hrozby.

Aktíva sa delia na:

- Hmotné (nehnuteľnosti, cenné papiere, peniaze apod.)
- Nehmotné (informácie, prestíž organizácie, morálka pracovníkov, kvalita personálu apod.).

Aktívom môže byť ale aj sám subjekt, nakoľko hrozba môže pôsobiť na celú jeho existenciu.

Aktívum motivuje útočníka k aktivácii hrozby. Voči pôsobeniu hrozby sa aktívum vyznačuje určitou zraniteľnosťou. Aktívum je chránené protiopatreniami pred hrozbami.

Zraniteľnosť

Zraniteľnosťou rozumieme nedostatok analyzovaného aktíva, ktorým môže dôjsť k naplneniu hrozby.

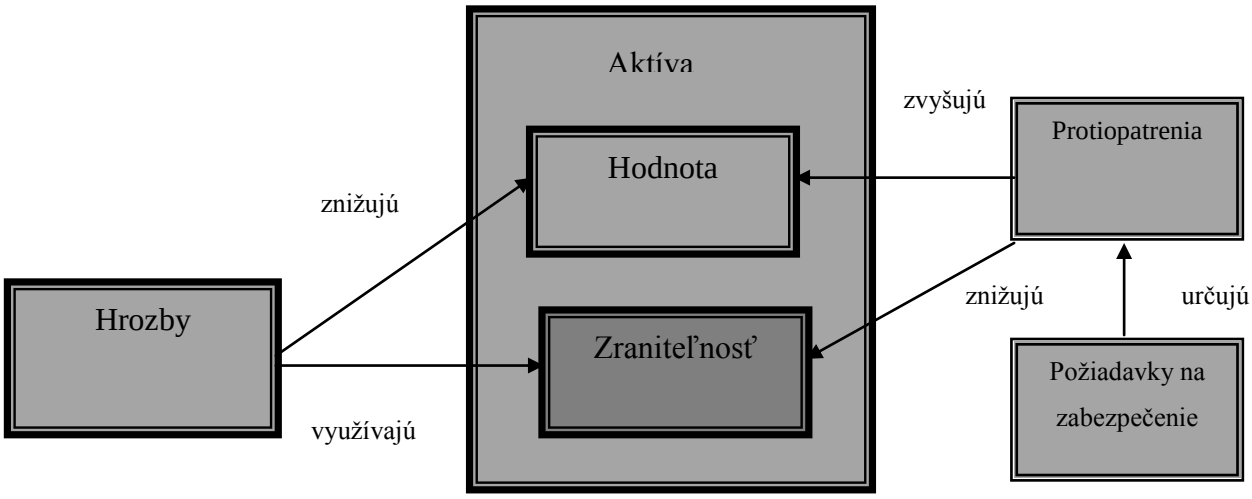
Zraniteľnosť je vlastnosťou rizika a vyjadruje, ako citlivé je aktívum na pôsobení danej hrozby. Vznikne tam, kde dochádza k interakcii medzi hrozbou a aktívom. Základnou charakteristikou zraniteľnosti je jej úroveň . Úroveň zraniteľnosti aktíva sa hodnotí podľa nasledujúcich faktorov:

Citlivosť – náchylnosť aktíva byť poškodené danou hrozbou,

Kritickosť – dôležitosť aktíva pre analyzovaný subjekt.

Vzájomné vzťahy medzi hrozbou, protiopatrením,

aktívom a zraniteľnosťou



Nástrojom , prostriedkom na vykonanie bezpečnostnej analýzy je dôkladná analýza rizík.

[9]

3.1 Analýza rizík

Analýza rizík je

- prvým krokom procesu znižovania rizikových situácií,
- proces definovania hrozieb, pravdepodobnosti ich výskytu a dopadu na aktíva, teda stanovenie rizík a ich závažnosti,
- základným vstupom pre riadenie rizík ako nadväzujúca činnosť.

Analýza rizík s cieľom určenia stupňa zabezpečenia (ČSN EN 50131-1)

Stupeň 1: Nízke riziko

Predpokladá sa, že narušiteľ má malú znalosť I&HAS (poplachový zabezpečovací a tiesňový systém) a má k dispozícii obmedzený sortiment dostupných nástrojov.

Stupeň 2 : Nízke až stredné riziko

Predpokladá sa, že narušiteľ má obmedzenú znalosť I&HAS a používania bežného náradia a prenosných prístrojov.

Stupeň 3 : Stredné až vysoké riziko

Predpokladá sa, že narušiteľ je oboznámený s I&HAS a má rozsiahly sortiment nástrojov a prenosných elektronických zariadení.

Stupeň 4 : Vysoké riziko

Používa sa , ak má zabezpečenie prioritu pred všetkými ostatnými hľadiskami. Predpokladá sa, že narušiteľ je schopný alebo má možnosť spracovať podrobný plán vniknutia a má kompletný sortiment zariadení vrátane prostriedkov pre náhradu rozhodujúcich komponentov I&HAS.

3.2 Postup pri spracovaní analýzy rizík

3.2.1 Určenie hranice analýzy rizík

Pri určení hranice analýzy sa vychádza zo zámeru vlastníka objektu, prípadne z úvodnej štúdie, ak bola spracovaná.

Aktíva, ktoré majú vzhľadom k prebiehajúcemu procesu znižovania rizík vzťah k cieľom vlastníka, budú zahrnuté do analýzy a budú ležať vnútri hranice analýzy.

Ostatné aktíva budú ležať mimo hranice analýzy rizík.

3.2.2 Identifikácia aktív

Identifikácia spočíva vo vytvorení súpisu všetkých aktív ležiacich vnútri hranice analýzy rizík. Pri rozhodovaní o zaradení daného aktíva na súpis sa uvedie názov aktíva a jeho umiestnenie.

3.2.3 Stanovenie hodnoty a zoskupovanie aktív

- Stanovenie hodnoty je založené na veľkosti škôd, ktoré boli spôsobené zničením či stratou aktíva.
- Vychádza z nákladových charakteristík (zriaďovacia cena atď.).
- Vlastnosti aktíva, slúžiace k dosiahnutiu ziskov nepriamo – napríklad postavenie na trhu, ochranná známka, ale aj kvalifikácia a know-how zamestnancov.
- Potreba rozlíšiť, či sa jedná o jedinečné aktívum alebo o aktívum jednoducho nahraditeľné.
- Do hodnoty sa premieta aj závislosť subjektu na existencii, ale i na správne fungovanie hodnoteného aktíva, teda k akým škodám dôjde obmedzením funkčnosti alebo stratou aktíva, než dôjde k jeho obnove.

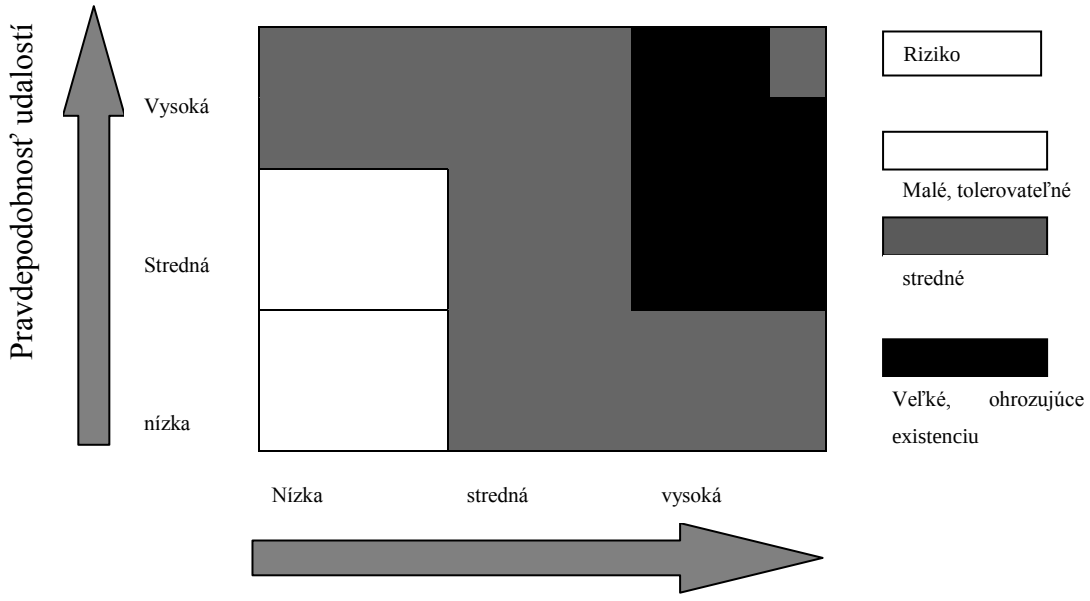
3.2.4 Identifikácia hrozieb

- Vykonanie výberu hrozieb, ktoré by mohli ohroziť minimálne jedno z aktív subjektu.
- Možno vychádzať zo zoznamu hrozieb, zostavených podľa zozbieraných informácií, vlastných skúseností, prieskumov vykonaných analýzami.
- Hrozby sa môžu odvodzovať tiež od subjektu, jeho statusu, postavenia na trhu, hospodárskych výsledkov, zámeru podnikateľa.
- Vykonáva sa pomocou metódy napr. brainstorming, Delphi a pod.

3.2.5 Analýza hrozieb a zraniteľnosti

- Každá hrozba sa hodnotí voči každému aktívu.
- U tých aktív, na ktorých sa hrozba môže uplatniť, sa určí úroveň hrozby voči tomuto aktívu a úroveň zraniteľnosti aktíva voči tejto hrozbe.
- Pri stanovení úrovne hrozby sa vychádza z faktorov ako nebezpečnosť, motivácia a prístup.
- Pri stanovení úrovne zraniteľnosti sa vychádza z faktorov ako citlivosť a kritickosť.
- Pri analýze úrovne hrozieb a zraniteľnosti sa berú do úvahy realizované protiopatrenia.
- Tieto protiopatrenia môžu znížiť ako úroveň hrozby, tak aj úroveň zraniteľnosti.
- Výsledným stavom je zoznam dvojíc „hrozba - aktívum“ so stanovenou úrovňou hrozby a zraniteľnosti.

Matica rizika - príklad



3.2.6 Pravdepodobnosť javu

Určitý jav charakterizujeme tým, s akou pravdepodobnosťou môže tento jav nastať.

Analyzujeme, či je jav náhodný či naopak, či patrí do určitého intervalu, prípadne aké sú jeho pravdepodobnostné charakteristiky.

a) Nezávislé pravdepodobnostné javy

Pravdepodobnosť, s akou nastane určitý jav, nie je závislá na tom, aký jav nastal predtým

b) Podmienené pravdepodobnosťou (závislé javy)

Pravdepodobnosť, s akou nastane určitý jav, je podmienený výskytom iného javu.

3.2.7 Meranie rizika

Výška rizika vyplýva z hodnoty aktíva, úrovne hrozby a zraniteľnosti aktíva.

Pri analýze sa pracuje s veličinami, ktoré nemožno v mnohých prípadoch presne zmerať a určenie ich veľkosti spočíva na kvalifikovanom odhade špecialistu, vyjadrujúceho sa len na základe vlastných, dlhoročných skúseností, kde určí predpokladaný stupeň rizika.

[9]

3.3 Prostredie

Pri bezpečnostnej analýze je veľmi dôležité vyhodnotenie prostredia z hľadiska bezpečnosti, v ktorom objekty pôsobia a v ktorom prebieha koexistencia objektov a subjektov priemyslu komerčnej bezpečnosti na základe aktívneho alebo pasívneho záujmu. Môžu to byť :

- Záujmové objekty – budovy, hospodárske objekty, ktoré strážime, alebo ich technicky zabezpečujeme, alebo sú, boli, eventuálne môžu byť napadnuté páchateľmi krádežou vlámaním, teroristami apod. a predstavujú trvalý alebo dočasný záujem kriminálnych živlov.

- Priľahlé prostredie – záujmové objekty kriminálnych živlov s cieľom ukrytia, prípravy, alebo nástupu k napadnutiu objektu alebo predstavujúci záujem podnikov priemyslu komerčnej bezpečnosti z obdobných dôvodov, alebo z dôvodov technických a organizačných.
- Kriminálne prostredie – aglomerácia potenciálnych páchateľov kriminálne trestnej činnosti, ich pomocníkov a ukrývačov. Komunita kriminálne mysliacich osôb a ich stykov.
- Geografické prostredie – štúdium konkrétnej bezpečnostnej situácie v mieste, okrese, kraji, regiónu, reakcie na zmeny a analýzy.

3.3.1 Hodnotenie prostredia

Hodnotíme :

- **Zraniteľnosť prostredia** – je nutné venovať ochrane prostredia prvoradú pozornosť. Hlavne v chránených objektoch potom zraniteľnosť prenikania do objektu.
- **Vhodnosť prostredia** – analyzovať, či je prostredie vhodné pre nás, alebo kriminálne podsvetie. Pri hodnotení je potrebné urobiť jasný záver, prečo kriminálne podsvetie mohlo dosiahnuť úspechu, kto za to môže, čo je príčinou, či bol náš systém účinný. Pokiaľ nie, zvýšiť jeho účinnosť, spoľahlivosť, znížiť zraniteľnosť systému a následne vyvodiť záver napr. ku sprísneniu režimových opatrení, zvýšiť počet pracovníkov, zamedziť prístupnosť prostredia pre kriminálne živly.

[4]

4 BEZPEČNOSTNÁ PROGNÓZA

Budúcnosť sa vyznačuje vysokou mierou neurčitosti a prognózovanie umožňuje túto mieru neurčitosti znížiť. Čím presnejšie naše prognózovanie bude, tým jednoduchšie bude pre nás plánovanie. Význam prognózovanie tkvie v tom, že sa sústreďuje na predvídanie budúceho vývoja prostredia a na vznik podmienok, ktoré nastanú v budúcnosti, a ktoré budú mať vplyv na problém, ktorý riešime v súčasnosti. Prognózovanie je základom pre plánovanie a umožňuje nám posúdiť nami nevrhnuté alternatívne riešenia v kontexte s budúcim podnikaním. Využíva sa hlavne pre organizáciu ako celok, ale možno ju použiť pri riešení čiastočných problémov v jednotlivých činnostiach organizácie. Tiež v oblasti bezpečnosti organizácie má prognózovanie svoje nezameniteľné miesto.

Bezpečnostné prognózovanie sa vyznačuje určitými odlišnosťami oproti iným druhom prognózovania, ktoré sa v organizácii vykonávajú. Bezpečnostné prognózovanie je poznávací proces, ktorý sa zaoberá javmi a udalosťami, ktoré majú priamu i nepriamu väzbu na bezpečnosť organizácie a ktoré udávajú alebo výrazne ovplyvňujú smer nutného ďalšieho bezpečnostného vývoja organizácie v sledovanom čase.

Porovnaním realizácie plánovaného priebehu so skutočným bývajú často odhalené významné odchýlky. Po analýze príčin týchto odchýlok možno tieto informácie použiť pre korekciu pôvodnej prognózy.

Významnou odlišnosťou od iných druhov prognóz je skutočnosť, že v oblasti zabezpečenia organizácie pracujeme hlavne s informáciami, javmi a udalosťami, ktoré možno čiastočne kvantifikovať, čo významne ovplyvňuje výber prognostických metód. Ani obvyklé členenie prognostických metód na kvalitatívne a kvantitatívne nám neuľahči voľbu, nakoľko niektoré kvalitatívne metódy vychádzajú a produkujú číselné výsledky, a opačne niektoré kvantitatívne metódy vychádzajú zo subjektívnych hľadísk hodnotenia.

Medzi kvalitatívne metódy patria hlavne osobné hodnotenie, panelová zhoda a metóda Delphi. Medzi kvantitatívne metódy, ktoré môžeme použiť v rámci bezpečnostnej prognózy sú projektovanie trendov, a to metóda kĺzavých priemerov a exponenciálne vyrovnávanie.

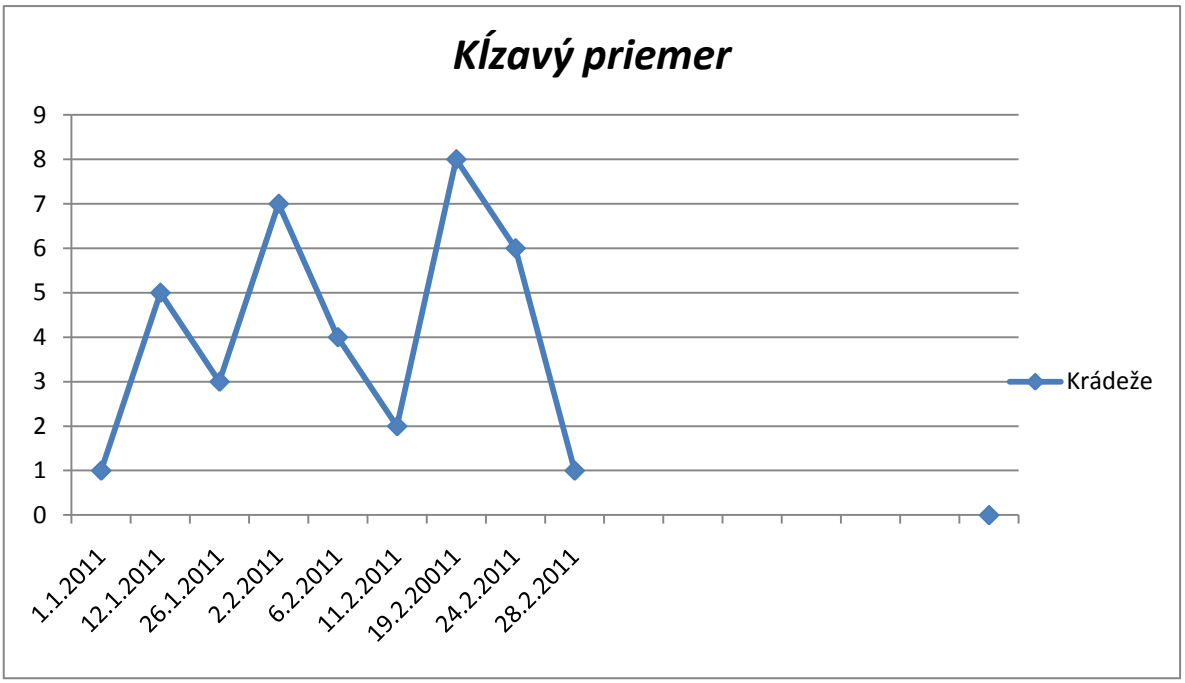
Osobné hodnotenie - je v praxi najčastejšie používanou metódou. Podstata metódy spočíva v tom, že jednotlivec predvída subjektívne budúcnosť. I keď jej spoľahlivosť a presnosť je sporná, v mnohom záleží na odbornosti a skúsenosti jednotlivca, ktorý

predpovedanie vykonáva, možno ju použiť tam, kde nie sú k dispozícii štatistické dáta. Používa sa najmä pre krátkodobé predpovede, skôr prevádzkového charakteru.

Panelová zhoda – čiastočne obmedzuje vplyv osobných postojov a myšlienkových stereotypov prognózujúceho jednotlivca tým, že subjektom, ktorý predpovedanie vykonáva, nie je jednotlivec, ale kolektív. Malo by sa jednať o kolektív jednotlivcov, ktorí majú určitú odbornú úroveň a znalosť bezpečnostnej problematiky a oblasti komerčnej bezpečnosti zvlášť. Vzájomným zdieľaním svojich názorov a postojov dospieť k zhode, prezentujúcej predpokladaný vývoj.

Metóda Delphi – využíva úsudok kolektívu odborníkov. Členovia tímu nevykonávajú prognózovanie spoločne, ale oddelene. Ani im nie je známe, kto sú ostatní členovia tímu. Hodnotenie vyplňuje každý odborník samostatne do pripraveného dotazníka. Dotazníky sa zozbierajú, sumarizujú a vrátia späť expertom, pričom má každý možnosť svoje pôvodné stanovisko revidovať s ohľadom na názor ostatných členov tímu. Takto sa postupuje tak dlho, dokiaľ sa nedosiahne obecnej zhody alebo dokiaľ nie je vykonaný príslušný počet vopred dohodnutých kôl hodnotenia. Nevýhodou tejto metódy je časová a organizačná náročnosť. Výhodou je anonymita účastníkov.

Metódy kĺzavých priemerov – táto metóda patrí medzi prognostické metódy kvantitatívne a možno ju použiť aj v oblasti bezpečnostného prognózovania. Predstavme si, že by sme radi zistili, aký je doterajší vývoj nejakej veličiny, a na základe toho predpovedali jej budúci vývoj. Napr. môžeme túto metódu použiť pre prognózu počtu krádeží tovaru v obchodnom dome. Výsledkom je grafické znázornenie napr. v podobe lineárneho spojnicového grafu, kde na zvislú os vynesieme údaje o počte krádeží a na os vodorovnú jednotlivé dni, kedy došlo ku krádežiam. Pokiaľ sledujeme len krátke obdobie, napr. niekoľko málo týždňov, potom prognóza vývoja je v podstate aritmetickým priemerom hodnôt z predošlých týždňov (2-3). Akonáhle však pre predpoveď vývoja v nasledujúcom týždni by sme mali použiť veľkého počtu predošlých týždňov, nie sme schopní vziať do úvahy napr. výrazné zmeny, ku ktorým došlo v najbližších predošlých týždňoch. Preto sa nepoužíva bežný aritmetický priemer zo všetkých predošlých období, ale tzv. priemer kĺzavý, tzn. priemer z vopred stanoveného počtu posledných týždňov. Tento spôsob je použiteľný skôr na krátkodobé predpovede.



Metóda exponenciálneho vyrovnania – upresňuje metódu kĺzavého priemeru tak, že odlišuje význam jednotlivých údajov podľa toho, či sa jedná o údaje novšie alebo staršie. Pre presnejšiu prognózu v mnohých prípadoch majú väčší význam dáta novšie než dáta staršie. V princípe ide o výpočet váženého kĺzavého priemeru skutočných hodnôt, kde aktuálnejšie hodnoty majú väčšiu váhu ako ostatné.

[1]

4.1 Prognózovanie bezpečnostnej situácie

V tomto smere získavame údaje o pravdepodobnom vzťahu všetkých článkov v budúcnosti, skúmame vývojové perspektívy rôznych javov. Ide o predvídanie vývoja bezpečnostnej situácie, alebo bezpečnostných javov, a to na základe analýzy, obecnej a analogickej syntézy. Prognóza sa vykonáva na základe predvídania pravdepodobných zmien a doby, kedy sa asi uskutoční. Bez tohto predvídania nemôžeme ofenzívne klásť odpor kriminálnemu prostrediu. Prognózovania sa musí dotýkať všetkých článkov bezpečnostnej situácie, musíme predvídať , ako bude kriminálne prostredie jednať. Je nutné si uvedomiť, že pokiaľ sa kriminálnemu prostrediu podarí dosiahnuť určitého úspechu, bude vo svojej činnosti pokračovať.

Prognózovanie je úzko späté s plánovaním. Prognózovanie umožňuje zistiť, čo sa môže stať v budúcnosti a za akých podmienok. Pre plánovanie našej činnosti je najdôležitejšie poznania tendencie vývoja. Pri prognózovaní sa používajú aj nasledovné metódy :

1) **Využitie doterajších skúseností**

Hlavne naše chyby, ktorých sme sa dopustili, je ale nutné vedieť, že tiež kriminálne prostredie, ale predovšetkým organizovaný zločin sa učí z našich chýb a rovnako neustále analyzuje , takže nie je možné všetko bezmyšlienkovite aplikovať. Je treba analyzovať, čo môže náš protivník všetko vedieť o spôsobe zaistenia našich zákazníkov.

2) **Využitie tendencií rozvoja**

Sú využívané informácie, štatistické údaje a závery o činnosti kriminálneho prostredia, špecializácia našich pracovníkov a to jak z fyzickej , tak aj technickej ochrany, ďalej skúsenosti z nasadzovania technických prostriedkov priemyslu komerčnej bezpečnosti, ale i skúsenosti z prekonávania týchto prostriedkov kriminálnym podsvetím a organizovaným zločinom.

3) **Modelovanie bezpečnostných situácií**

Vychádzajúc z doterajších skúseností sú vytvárané modely rôznych typov bezpečnostných situácií. Napr. modely činnosti kriminálneho prostredia, modely možného prekonania zabezpečeného objektu, model hasičského útoku ku zdolaniu požiaru, model evakuácie dielne zasiahnutej nebezpečnou chemikáliou, model napadnutia bankovej pobočky, model zaistenia a obranných opatrení pri prepadnutí transportu peňazí atď.

4) **Znalecké hodnotenie**

Spolupracuje sa pracoviskami skúšobníctva v obore priemyslu komerčnej bezpečnosti, hlavne v oboroch elektrických a mechanických zabezpečovacích systémoch. Využívajú sa aj experti certifikačných ústavov a inštitútov, súdnych znalcov, expertov vedeckých a výskumných ústavov, vrátane zahraničných odborných inštitúcií apod.

[4]

5 BEZPEČNOSTNÉ PLÁNOVANIE

5.1 Plánovanie ako funkcia riadenia, druhy plánovania

Podstata plánovania spočíva v koordinácii našich úloh v podmienkach priemyslu komerčnej bezpečnosti. Vykonáva sa štúdium bezpečnostnej situácie, stanovenie bezpečnostných rizík, analýza a syntéza a výsledky je treba vziať do úvahy pri následnom plánovaní našej činnosti.

Pri plánovaní má vždy prvoradú prednosť chránený záujem zákazníka. Plánovací proces musí rešpektovať platné zákony, nariadenia, predpisy a etiku bezpečnostnej práce.

Metodologický základ plánovania

Plánovanie je nutné chápať ako predvídanie budúceho rozvoja priemyslu komerčnej bezpečnosti. Je treba používať vedecké metódy práce, kvalifikovanú prognózu a futurologiu. Odlišnosť plánovacieho procesu v priemysle komerčnej bezpečnosti je hlavne v tom, že je treba prihliadať k aktuálnej bezpečnostnej situácii v ktorej sa nachádzame, priebežne ju analyzovať a na základe toho potom priebežne plánovaciu činnosť, vrátane plánovacích dokumentov spresňovať a doplňovať. Dôležitá je to prognóza tzn. predvídanie a modelovanie vývoja bezpečnostnej situácie. Súčasný problém spočíva v tom, že sa tieto otázky podceňujú s výhovorkou, že ne nie je čas, nie sú ľudia a finančné prostriedky. Tým sa môže stať, že naša činnosť môže za krátky čas vykazovať prvky diletantizmu. Bez kvalitnej prognózy nemôže byť ani kvalitného plánovania. Pri plánovacej činnosti je treba brať do úvahy objektívne zákonitosti priemyslu komerčnej bezpečnosti na ktorých základoch podnikáme. Je treba rešpektovať tieto zákonitosti a poznávať ich mechanizmus. Študujeme teda každý prvok bezpečnostnej situácie a činnosti zúčastnených objektov i subjektov v priemysle komerčnej bezpečnosti.

Podstatou plánovacej činnosti v priemysle komerčnej bezpečnosti je vytvorenie vedecky odôvodneného programu činnosti systému aparátu priemyslu komerčnej bezpečnosti v záujme dosiahnutia stanoveného cieľa

Z tejto definície vyplýva, že plánovanie nesmie byť súhrn opatrení, ale musí sa tu prejaviť cieľavedomosť. S plánom je treba priebežne pracovať, hlavne v smere spresňovania cieľov. Skutočný plán musí byť pružný, to znamená, že sa v ňom musia robiť korekcie.

S pomocou plánovania manažér riadi činnosť podriadených subjektov, ale i objektov. V tom spočíva funkcia riadenia. Ako funkcia plánovania je plán základňou pre ďalšiu činnosť. Plán obsahuje i smery tejto činnosti, ktorá sa bude vykonávať a to konkrétne sformulované.

Úloha plánovania spočíva v tom, že:

- Zabezpečuje výber, stanovenie cieľov.
- S pomocou plánovania vyhľadávame účinnejšie cesty a spôsoby dosiahnutia týchto cieľov.
- S pomocou plánu určujeme potrebné množstvo síl a prostriedkov k ich dosiahnutiu a tiež určujú spôsoby optimálneho rozmiestnenia síl a prostriedkov.
- S pomocou plánu sa zabezpečuje koordinovanosť všetkých článkov a prvkov systému priemyslu komerčnej bezpečnosti.

Plány delíme podľa druhov na :

- Obecné plány – plán činnosti jednotlivých výkonných pracovníkov.
- Čiastočné plány – plán prípadu u polície, detektívne služby, previerky, stráženie budovy. Závisí na rozsahu a dôležitosti.
- Perspektívne plány – výhľadové

Tie môžu byť spracované na 5-10 rokov. Cieľ je vytvoriť potrebné materiálové rezervy, rezervy ľudských zdrojov dlhodobo školených, vychovávaných a vycvičovaných. Postupné budovanie technických ochranných či zabezpečovacích systémov. S pomocou perspektívneho plánovania vytvárame jednotnú formu činnosti v priemysle komerčnej bezpečnosti. Nemôžeme pripustiť, aby kriminálne podsvetie a organizovaný zločin boli v ofenzíve a my to len defenzívne sledovali.

- Priebežné plány

Ide v praxi o najviac používaný plánovací postup. V priemysle komerčnej bezpečnosti je treba spracovávať ročné plány školenia, technického zabezpečenia, technického výcviku. Práca podľa konkrétnych plánov k jednotlivým akciám sa ukázali ako účinný nástroj riadenia. Ako pružný nástroj riadenia sa ukázali kvartálne plány, hlavne u technických zložiek priemyslu komerčnej bezpečnosti.

5.2 Získavanie východiskových údajov pre plánovanie

Východiskové údaje potrebné pre plánovanie získavame analýzou našej činnosti a analýzou bezpečnostnej situácie na základe vyhodnotenia bezpečnostných rizík a vykonanej syntézy vzniknutých vstupných informácií. Ďalej získaním faktických údajov z bezpečnostnej situácie zistených na obhospodarovanom úseku činnosti priemyslu komerčnej bezpečnosti.

5.3 Metodika a formy plánovania

Metodika plánovania

- **Odsúhlasovanie plánu**

Každý bod plánu má byť v súlade s bezpečnostnou politikou podniku. V každom pláne musia byť postavené úlohy reálne vyplývajúce z bezpečnostnej situácie, každý novo vytvorený plánovací dokument musí byť logicky spojený so starým plánovacím dokumentom.

Plány je nutné koordinovať i v rámci niekoľkých pracovísk jednej bezpečnostnej firmy, alebo plánovanú súčinnosť je nutné koordinovať s políciou, hasičských záchranným zborom, mestskou políciou atď. Až potom je možno plánovací dokument odsúhlasiť zodpovedným pracovníkom.

- **Optimalizácia plánovacích dokumentov**

Systém plánovania – pyramída. Plán je spracovávaný od hora nadol, a tak sa i plní, vrátane zodpovednosti. Avšak podklady musia prísť z dolu od výkonných pracovníkov. Iný systém je tzv. komplexné plánovanie, kedy plány spracovávajú jak podriadené, tak nadriadené pracoviská a potom sa kompletizujú a optimalizujú.

Existujú dve formy plánov:

- Popisná forma – najoptimálnejšia, všetko sa pracovník dočíta, čo má robiť, ako to má robiť, kedy to má robiť

- Grafická forma – momentálne je na vzostupe, vďaka informačnej technológii, je výhodná pre okamžitú prehľadnosť a v podstate jednoduchosť pochopenia napr. plán služieb, plán prevozu peňazí atď.

Stredisko: **HARMONOGRAM VÝKON FYZICKEJ OCHRANY za mesiac/rok: I./2011**

FUN	MENO	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	ODPR. HOD.	Podpis pracovníka
I.	PRAC. ZMENY	R	R			N	N			R	R			N	N			R	R			N	N			R	R			N	N			
Čl. 1																																	197,5	
II.	PRAC. ZMENY	N	N			R	R			N	N			R	R			N	N			R	R			N	N			R	R			
Čl. 1																																	211,5	
III..	PRAC. ZMENY			R	R			N	N			R	R			N	N			R	R			N	N			R	R			N		
Čl. 1																																	173,5	
IV.	PRAC. ZMENY			N	N			R	R			N	N			R	R			N	N			R	R			N	N			R		
Čl. 1																																	208,5	

PD – R - 06,00 – 15,30 = 9,5 h **So,Ne,Sv – R - 06,00 – 18,00 = 12 h**

N - 13,30 – 06,00 = 16,5 h **N – 18,00 – 06,00 = 12 h**

Plánovací dokument má spravidla štyri časti:

1. Krátka bezpečnostná situácia a základné trendy vývoja

V každej podnikovej jednotke existuje ako samostatný dokument spolu s príručkou.

2. Úlohy, ktoré majú byť vykonané

Vyplývajú zo zákona, bezpečnostnej doktríny, smerníc a predpisov apod. Obyčajne tu majú byť hlavné úlohy.

3. Základné bezpečnostné opatrenia

Vykonávané opatrenia v rámci firmy, v objektoch zverených k stráženiu a ochrane, k technickému zabezpečeniu a dohľadu, eventuálne, kde bude vykonávaný transport peňazí a cenín, bodyguarding apod. Plánujú sa i opatrenia súčinnostného charakteru, upevňujúce spoluprácu s verejnosťou apod., preventívna činnosť, analytický prieskum atď.

V každom bode plánu je uvedená zodpovedná osoba. Ďalej termíny priebežnej kontroly a termín realizácie záverečnej kontroly, odovzdávací protokol, záručný list apod..

4. Organizačné opatrenia

Je v plánoch manažérov jednotlivých služieb a vyšších riadiacich článkov. Je tu vyznačené vykonávanie kontrol, organizácia kontrol, sledovanie skúšok a revízií, výcviku a školení, tréningov strelieb, fyzických a odborných previerok, inšpekcií, auditov.

[4]

6 BEZPEČNOSTNÁ POLITIKA

Bezpečnostná politika organizácie je súhrn odpovedí vrcholového vedenia organizácie hlavne na tri otázky:

- Čo má organizácia v oblasti bezpečnosti konať a z akého dôvodu
- Akých cieľov v oblasti bezpečnosti chce dosiahnuť
- Ako bude riadiť jednotlivé podnikové činnosti a aké vykoná opatrenia , aby boli stanovené ciele dosiahnuté.

Aby bezpečnostná politika skutočne mohla plniť svoj účel a stala sa účinným nástrojom k presadeniu bezpečnostných opatrení a zásad v nej obsiahnutých, mala by byť vyjadrená v písomnej forme. Dokument bezpečnostnej politiky má charakter všeobecného plánu pre oblasť bezpečnosti organizácie a má veľmi obecný charakter. Z hierarchie celkových záujmov a cieľov organizácie vyplýva, že bezpečnostná politika musí byť podriadená obecnej politike organizácie, tzn. jej obecnému strategickému plánu. Formulácia prehlásení v dokumente bezpečnostnej politiky sú obecné, zaberajú celú šírku danej problematiky vnútri organizácie a ako také nemôžu byť bez ďalšieho rozpracovania použité k priamej realizácii. Rozhodujúcim spôsobom určuje smer a spôsob ďalšieho konania organizácie v danej oblasti.

V dokumente bezpečnostnej politiky organizácie je zodpovedané množstvo ďalších otázok, ako napr.:

- Kto nesie zodpovednosť za plnenie záverov bezpečnostnej politiky,
- Aký je časový horizont pre naplnenie cieľov bezpečnostnej politiky,
- Ako bude bezpečnostná politika uvádzaná do praxe,
- Aké sú na bezpečnostnú politiku kladené požiadavky z hľadiska efektivity a nákladov,
- Ako bude dodržovanie bezpečnostnej politiky vynucované, príp. sankcionované v prípade porušenia.

Pretože problematika bezpečnosti organizácie je veľmi široká a zameriava sa na tri základné oblasti – ľudí, majetok a informácie, bude i obecná bezpečnostná politika organizácie musieť riešiť problematiku uvedených troch oblastí, pre ktoré sa formuluje samostatná bezpečnostná politika:

- V oblasti personálnej
- V oblasti organizačnej a administratívnej
- V oblasti ochrany majetku – hmotného majetku
- Politika ochrany nehmotného majetku
- V oblasti informačných systémov

Vo vzťahu k bezpečnostnému projektu je treba uviesť , že bezpečnostný projekt je konkretizáciou opatrení a podrobným plánom realizácie zásad a cieľov stanovených bezpečnostnou politikou.

Na rozdiel od bezpečnostnej politiky je bezpečnostný projekt veľmi konkrétny a podrobný, zameraný na každý detail, a to vrátane sledovania nákladov na realizáciu.

[1]

SBS Trenčín, spol. s ručením obmedzeným

BEZPEČNOSTNÁ POLITIKA

Manažment spoločnosti SBS Trenčín, spol. s r.o.. vedomý si svojej zodpovednosti za kvalitu, vyhlasuje svoju Politiku kvality s nasledovnými princípmi:

1. ***Spokojnosť zákazníka je našou najvyššou prioritou.***
2. *Pružnosť realizačného programu, vysoká kvalita všetkých činností a produktov v oblasti poskytovania strážnej služby, prepravy finančných prostriedkov a cenín sú predpokladom na upevnenie a neustále zlepšovanie nášho postavenia na domácom trhu.*
3. *Kvalita je prvá a základná úloha za splnenie ktorej zodpovedajú zamestnanci spoločnosti na všetkých riadiacich a výkonných miestach.*
4. *Zaväzujeme sa spĺňať požiadavky a trvalo zlepšovať efektívnosť systému manažérstva kvality.*
5. *Dodávateľov výstroje, výzbroje a služieb aktívne začleňujeme do nášho systému manažérstva kvality.*
6. *Náš systém je účinný, ekonomický a prijateľný pre orgán poverený odberateľom, ktorý je uvedený v zmluve alebo ním povereného zástupcu, „Zástupca pre štátne overovanie kvality".*
7. *Zástupcovia vedenia organizácie majú potrebnú právomoc a organizačnú voľnosť na riešenie závažných problémov, ktoré súvisia s kvalitou.*
8. *Trvalé zlepšovanie systému manažérstva kvality je podporované a zabezpečované aktívnym prístupom zamestnancov na všetkých úrovniach spoločnosti.*
9. *Každý náš zamestnanec je reprezentantom spoločnosti a svojou prácou a vystupovaním pomáha budovať dobré meno spoločnosti a stabilizovať pozíciu spoločnosti u zákazníkov.*
10. *Starostlivosť o sociálne zabezpečenie, životné a pracovné prostredie je súčasťou stratégie rozvoja spoločnosti.*

7 BEZPEČNOSTNÝ PROJEKT

Bezpečnostný projekt sleduje maximálne odborne a kvalifikovane vyprojektovať určitý produkt podniku komerčnej bezpečnosti v súlade s prianiami zákazníka, akceptácii poisťovní, normotvorne ošetrený, certifikovaný a finančne prijateľný.

Bezpečnostný projekt je nevyhnutnou súčasťou dokumentácie bezpečnostnej ochrany akéhokoľvek objektu, kde je koncipovaná bezpečnostná politika.

Bezpečnostné projekty rozpoznávame:

1. Bezpečnostné projekty **obecné** eventuálne špeciálne– u štátu, kraja, regiónu, okresu, miesta, mesta. Musia obsahovať otázky zabezpečenia a bezpečnostnej ochrany republiky, kraja, regiónu atď. Ide väčšinou o projekty spracovávané štátnymi orgánmi, poprípade špeciálnymi štátnymi bezpečnostnými zložkami.
2. Bezpečnostné projekty **fyzickej ochrany** – riešia ochranu objektov, priestorov, lokalít, budov atď., ktorá je zaisťovaná fyzickou silou, teda pomocou strážnych služieb a ich sprievodných prostriedkov.
3. Bezpečnostné projekty **elektronickej ochrany** – obsahujú odborné projekty elektrických zabezpečovacích systémov, elektrickej požiarnej signalizácie, uzavretých strážiacich a dozorných systémov televíznych okruhov, elektronickej kontroly vstupov a dochádzkových systémov, elektronickej ochrany tovaru, elektronických integrovaných systémov, projekty pultu centralizovanej ochrany objektov a projekty integrovaných záchranných systémov.
4. Bezpečnostné projekty **detektívnej ochrany**
5. Bezpečnostné projekty **bodyguardingu** - rieši prípravu, personálne zabezpečenie a vlastné vykonanie osobnej ochrany. Obsahuje hlavne:
   - Určenie a analýzu bezpečnostných rizík zákazky
   - Zásady prijatia zákazky
   - Zhodnotenie dôvodov osobnej ochrany konkrétnej zákazky
   - Logistické zabezpečenie zákazky
   - Zásady prvej pomoci pri osobnej ochrane
6. Bezpečnostné projekty **prepravy peňazí a cenností** – sú bezpečnostné projekty špeciálneho charakteru. Musia obsahovať hlavne rozpracovanie zásad konkrétnej podmienky jednotlivej zákazky. Ide o zásady:

- Bezpečnosti
- Zodpovednosti
- Personalistiky
- Logistiky
- Efektivity nákladov
- Generálnej prevencie
- Organizačné zásady prepravy
- Psychologické aspekty prepravy

7. Bezpečnostné projekty mechanických zábranných prostriedkov a systémov – musí obsahovať:
    - Zhodnotenie bezpečnostných rizík
    - Analýzu súvzťažnosti
    - Syntézu a výstup pre plánovací činnosť

Bezpečnostné riziko v objekte určíme na základe vykonania bezpečnostno-technickej obhliadky.

Bezpečnostne technickú obhliadku vykonáme podľa nasledovných bezpečnostných zásad:

- Situácia - a)v objekte
  b)v priľahlom okolí
- taktické riešenie – podľa zistených situácii
  vlastným stanovením bezpečnostného rizika
- technické riešenie - vlastný popis – technologický popis riešenia
- spôsob vykonania mechanickej ochrany – montážny popis úkonov
- konfigurácia materiálu

Špeciálne objekty vyžadujú zaistenie podľa zákona 215/2004 Z.z. v znení neskorších predpisov O ochrane utajovaných skutočností, musia byť potom z hľadiska mechanických zábranných systémov zaistené podľa požiadaviek NBÚ. Tu v §54 zák. 215/2004 Z.z. je dané, že musia byť používané technické prostriedky certifikované národným bezpečnostným úradom, ale im poverenou organizáciou.

[3]

7.1 ZÁKON 215/2004 Z.z. o ochrane utajovaných skutočností

§ 54

Certifikácia mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov

(1) Mechanické zábranné prostriedky a technické zabezpečovacie prostriedky na ochranu utajovaných skutočností označených stupňom utajenia Dôverné a vyšším certifikuje úrad.
(2) Druhy certifikácie sú:

a) certifikácia typu mechanického zábranného prostriedku a certifikácia typu technického zabezpečovacieho prostriedku (ďalej len "certifikácia typu"),

b) certifikácia jednotlivého mechanického zábranného prostriedku a certifikácia jednotlivého technického zabezpečovacieho prostriedku (ďalej len "certifikácia prostriedku").

(3) O vydanie certifikátu typu žiada výrobca, dovozca alebo distribútor 21) úrad.
(4) O vydanie certifikátu prostriedku žiada užívateľ úrad.
(5) Certifikát typu alebo certifikát prostriedku sa udeľuje pre konkrétny stupeň utajenia a podmienkou jeho platnosti je dodržanie podmienok a pravidiel používania v ňom určených.
(6) Certifikát udelený na určitý stupeň utajenia platí aj pre nižší stupeň utajenia.
(7) Dobu platnosti certifikátu typu alebo certifikátu prostriedku určí úrad.
(8) Náklady spojené s certifikáciou uhrádza ten, kto o certifikáciu žiada.
(9) Mechanické zábranné prostriedky a technické zabezpečovacie prostriedky použité na ochranu
utajovaných skutočností môže užívateľ používať aj po skončení platnosti certifikátu typu v súlade s
podmienkami, ktoré ustanoví úrad.
(10) Ak úrad zistí, že mechanický zábranný prostriedok alebo technický zabezpečovací prostriedok nemá vlastnosti ustanovené na ochranu objektov alebo chránených priestorov, zruší platnosť
certifikátu.
(11) Úrad sa splnomocňuje na vydanie všeobecne záväzného právneho predpisu, ktorým

ustanoví podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích
prostriedkov a o ich používaní.

[5]

7.2 Realizácia bezpečnostného projektu

Realizáciou bezpečnostného projektu je završená najdôležitejšia fáza bezpečnostnej politiky, a to je dosiahnutie vytýčených bezpečnostných cieľov. Okrem už uvedených postupov pri riadení projektu je v období realizácie projektu a v následnom období veľmi dôležitou úlohou jeho implementácia. Je to nesmierne citlivý proces adaptácie organizácie, ich jednotlivých zložiek a hlavne každého zamestnanca spoločnosti na zmeny vyvolané realizáciou projektu. Každá zmena vyvolá v organizácii zákonite aj ďalšie zmeny. Môžu to byť zmeny zanedbateľné, ale tiež zmeny zásadného charakteru, ktoré sa dotnú i činností , ktoré bezprostredne s bezpečnosťou organizácie nesúvisia. Zavedenie novej bezpečnostnej techniky alebo nových režimových opatrení pri fyzickej ochrane organizácie si vynútia aj zmeny v zabehnutých stereotypoch chovania všetkých zamestnancov. Tieto zmeny sa často na začiatku stretávajú s odporom, ale postupne ich začínajú brať všetci ako samozrejmosť a dávajú si otázku : „Ako sme mohli bez toho predtým fungovať?“ . Veľakrát si nové zmeny vynútia aj zmeny v organizačnej štruktúre organizácie, systéme odmeňovania, v interných predpisoch a pravidiel.

[1]

8 SYNTÉZA PROBLÉMU

Pod pojmom syntéza problému v priemysle komerčnej bezpečnosti rozumieme implementáciu zmien do systému ochrany, pri ktorej je poznané alebo definované určité fungovanie alebo chovanie systému a hľadá sa taká štruktúra systému, ktorá by bola pre toto chovanie, fungovanie adekvátna.

Vzájomné väzby medzi chovaním a štruktúrou systému je možné zaisťovať a zabezpečovať niekoľkými spôsobmi:

- Päta predstavuje opakované empirické pozorovanie vzťahov chovania a organizácie. Tento vzťah môže byť v celku správne odpozorovaný. U ekonomických systémov, kam priemysel komerčnej bezpečnosti bezpochybne patrí, je avšak komplikácia, že ide o náhodné systémy s kauzálnymi reťazcami v chovaní, kde teda empirické pozorovanie prináša skôr štatistické opakovanie rôznych typov väzieb medzi vstupmi a výstupmi než jednoznačné závery.
- Druhým stupňom je tzv. konštruktérsky prístup, pri ktorom existuje konštruktérsky výkres výstavby systému, teda predstava o jeho fyzickej realite. Nemusí tu ale dôjsť k pochopeniu toho, prečo je systém konštruovaný práve takto.
- Tým sa od predchádzajúceho stupňa líši inžiniersky prístup zahrňujúci projektovanie zložitých systémov určitého chovania, čo nie je možné zabezpečiť už bez pochopenia systému a určitej znalosti jeho teórie.
- Špica (najvyšší stupeň) je potom prístup teoretický či vedecký, tvoriaci súbory vedeckých znalostí o systéme, jeho organizácii, chovaní, väzbách medzi organizáciou a chovaním.

Z daných prístupov sú pre systémovú syntézu objektov najdôležitejšie posledné dva, i keď sa v nej používajú aj prvé dva, najčastejšie prvý najjednoduchší prístup. Ako perspektívny pre úlohy plánovania a organizácie sa javí tretí prístup, nazývaná niekedy tiež Systémové inžinierstvo alebo Bezpečnostné inžinierstvo.

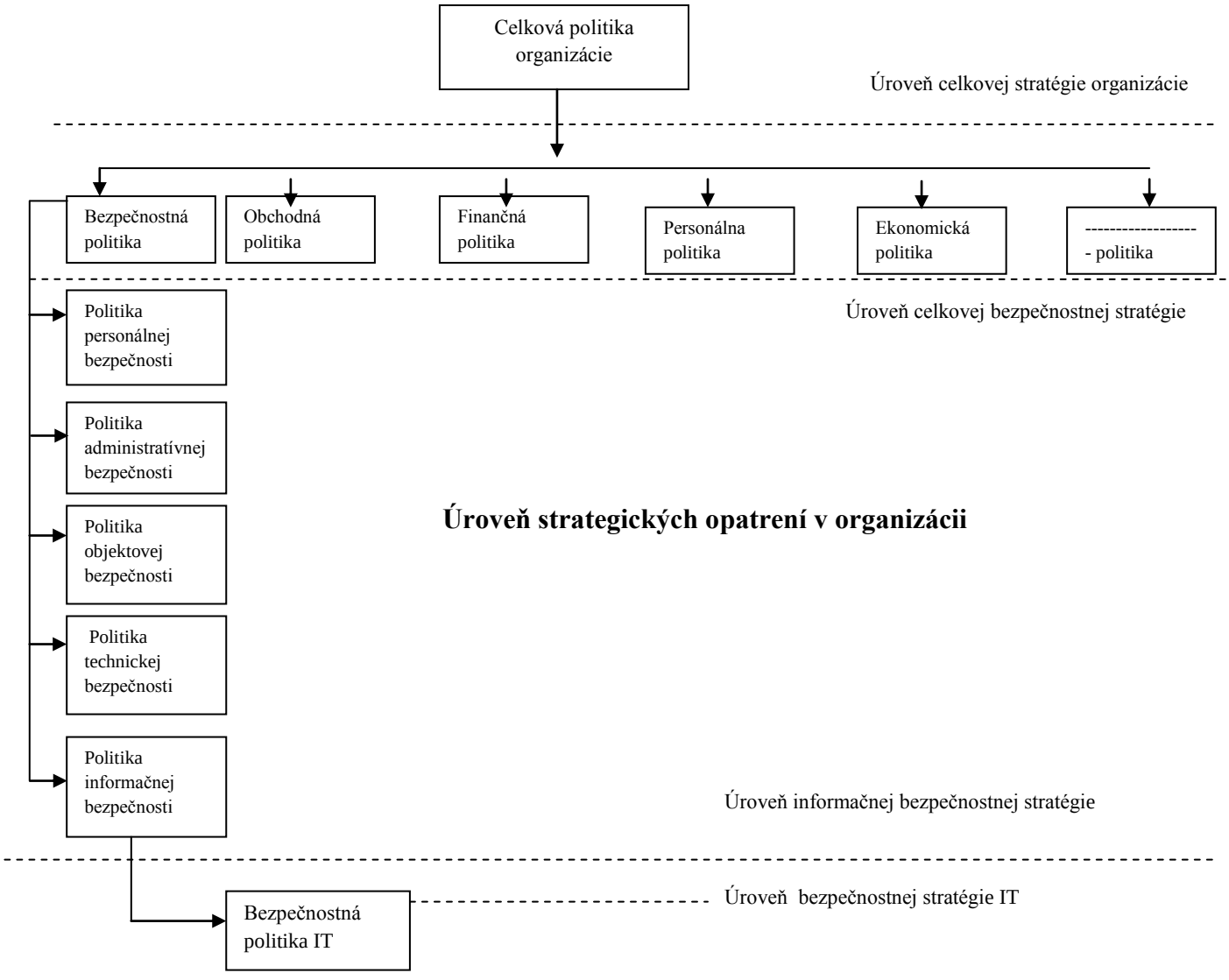
[4]

9 BEZPEČNOSTNÁ EXPERTÍZA A OCHRANA INFORMAČNÝCH TECHNOLÓGIÍ

Z hľadiska existencie a fungovania informačných technológií (IT) v organizácii je rozhodne žiaducim stavom bezpečnosť IT. Ako každý bezpečnostný cieľ organizácie je aj bezpečnosť IT výsledkom rady činností organizácie smerujúcich k jej dosiahnutiu a udržaniu. Ide teda o komplexný proces a je nutné poznamenať, že o proces veľmi zložitý.

Aj v prípade bezpečnosti IT je východiskom bezpečnostná politika. Pretože v rámci komplexnej bezpečnosti organizácie predstavuje bezpečnosť IT len časť bezpečnostnej problematiky, je i bezpečnostná politika IT časťou celkovej bezpečnostnej politiky organizácie.

Vzťah podradenosti bezpečnostnej politiky organizácie celkovej obecnej politike organizácie môžeme názorne vyjadriť aj graficky.



Z uvedeného je očividné , že základným východiskom pre bezpečnosť organizácie je celková politika organizácie. Pod pojmom informačná bezpečnosť organizácie rozumieme všetky bezpečnostné opatrenia slúžiace k ochrane informácií bez ohľadu na spôsob ich spracovania a uloženia (tzn. Bez ohľadu na to, či je informácia uložená na papieri, v elektronickej forme či inak).

Cieľom bezpečnostnej politiky IT je zaistiť bezpečnosť fungovania informačných technológií používaných v organizácii s ohľadom na bezpečnosť informácii do tohto systému vstupujúcich, v ňom obsiahnutých a z neho vystupujúcich, tzn. vo svojej podstate predísť, eliminovať, minimalizovať, popr. Iným spôsobom prekonať hrozby a riziká, ktorým môže byť informačná technológia organizácie reálne vystavená, aby organizácia neutrpela významnú ujmu.

Obsah bezpečnostnej politiky IT je podobný ako u celkovej bezpečnostnej politiky organizácie, a tak bezpečnostná politika IT sa spravidla musí zaoberať a riešiť:

- Cieľ bezpečnostnej politiky IT
- Popis informačnej technológie a hodnotenie jej významu pre fungovanie organizácie
- Legislatívne východiská
- Definovať kategórie významu informácií
- Definovať možné hrozby a riziká pôsobiace na IT
- Zásady personálnej politiky týkajúce sa IT
- Zásady organizačne administratívnych opatrení platných pre IT
- Technicko-prevádzkové zabezpečenie IT
- Politiku zálohovania dát
- Riešiť obnovu IT v období po prípadnej havárii
- Určiť metodiku riešenia kríz a mimoriadnych situácií.

Komplexné riešenie bezpečnosti IT organizácie predstavuje vykonanie:

- Komplexnej bezpečnostnej expertízy informačnej bezpečnosti
- Celková bezpečnostná analýza IT
- Analýza rizík
- Formulácia alternatív riešenia
- Projekt bezpečnosti IT a jeho realizácia.

Jedným zo základných kritérií IT je, aby vyhovoval podmienkam stanoveným obecne platnými právnymi predpismi, technickými normami a obecne užívanými štandardmi.

V rámci bezpečnostného procesu IT musí vzniknúť písomný dokument- bezpečnostná smernica, ktorý predstavuje komplex pravidiel pre bezpečné užívanie IT v praxi. V smernici musí byť jednoznačne stanovené:

- Kto zodpovedá za konkrétne druhy bezpečnosti IT na pracoviskách organizácie
- Chovanie užívateľov IT používaní IT
- Oprávnený prístup užívateľov k informáciám v IT
- Zriaďovanie a vedenie záznamov a písomností v súvislosti s užívaním IT
- Antivírové opatrenia
- Prístupová matica (tabuľka s vyznačením oprávnených subjektov a ich oprávnenia k práci s určitým objektom IT a povolený spôsob tejto práce)
- Postupy pri vytváraní nových užívateľských účtov a rušení neplatných
- Činnosť pri haváriách
- Ďalšie smernice, ak je to nevyhnutné.

[1]

10.1 Elektronický podpis

Pri ochrane informácií sa v súčasnej dobe veľmi rozrástlo používanie elektronického podpisu. Je to komplexné zabezpečenie dokumentov voči zasahovaniu neoprávnených osôb.

Zákon Slovenskej republiky č. 215/2002 Z.z. o elektronickom podpise definuje nasledovné:

§ 3

Elektronický podpis

(1) Elektronický podpis je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:

a) nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu,

b) na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie.

(2) Podpisovateľ vyhotoví elektronický podpis elektronického dokumentu tak, že na základe svojho súkromného kľúča a elektronického dokumentu vyhotoví nový údaj, ktorý spĺňa podmienky podľa odseku 1.

§ 4

Zaručený elektronický podpis

(1) Zaručený elektronický podpis je elektronický podpis, ktorý musí spĺňať podmienky podľa § 3:

a) je vyhotovený pomocou súkromného kľúča, ktorý je určený na vyhotovenie zaručeného elektronického podpisu,

b) možno ho vyhotoviť len s použitím bezpečného zariadenia na vyhotovovanie elektronického podpisu podľa § 2 písm. h),

c) spôsob jeho vyhotovovania umožňuje spoľahlivo určiť, ktorá fyzická osoba zaručený elektronický podpis vyhotovila,

d) na verejný kľúč patriaci k súkromnému kľúču použitému na vyhotovenie zaručeného elektronického podpisu je vydaný kvalifikovaný certifikát.

(2) Zaručený elektronický podpis je platný, ak

a) existuje kvalifikovaný certifikát verejného kľúča patriaceho k súkromnému kľúču použitému pri vyhotovení daného elektronického podpisu,

b) je preukázateľné, že kvalifikovaný certifikát podľa písmena a) bol platný v čase vyhotovenia daného elektronického podpisu,

c) elektronický dokument, ku ktorému je zaručený elektronický podpis pripojený alebo s ním inak logicky spojený, je zhodný s dokumentom použitým na jeho vyhotovenie, čo sa overilo použitím verejného kľúča uvedeného v kvalifikovanom certifikáte podľa písmena a).

(3) Podpisovateľ vyhotoví zaručený elektronický podpis elektronického dokumentu tak, že na základe svojho súkromného kľúča a daného elektronického dokumentu vyhotoví pomocou bezpečného zariadenia na vyhotovenie elektronického podpisu nový údaj, ktorý spĺňa podmienky podľa odseku 1.

(4) Formát a spôsob vyhotovovania zaručeného elektronického podpisu ustanoví všeobecne záväzný právny predpis, ktorý vydá úrad.
(5) Verejný kľúč patriaci k súkromnému kľúču určenému na vyhotovovanie zaručeného elektronického podpisu úradu je zverejnený spôsobom, ktorý ustanoví všeobecne záväzný právny predpis, ktorý vydá úrad.
(6) Zaručený elektronický podpis úradu je platný, ak elektronický dokument, ku ktorému je zaručený elektronický podpis pripojený alebo s ním inak logicky spojený, je zhodný s dokumentom použitým na jeho vyhotovenie, čo sa overilo použitím verejného kľúča úradu zverejneného spôsobom podľa odseku 5.

§ 5

Používanie elektronického podpisu

(1) Ak možno v styku s verejnou mocou používať elektronický podpis, tento elektronický podpis musí byť zaručeným elektronickým podpisom.
(2) Overovateľ overuje elektronický podpis prostriedkami na overovanie elektronického podpisu využitím podpísaného elektronického dokumentu a verejného kľúča patriaceho udávanému podpisovateľovi.
(3) Pri overovaní elektronického podpisu overovateľ môže požadovať overenie pravosti verejného kľúča, to znamená toho, že verejný kľúč patrí podpisovateľovi. Na tento účel môže použiť certifikát verejného kľúča podpisovateľa.
(4) Pri overovaní zaručeného elektronického podpisu overovateľ na základe kvalifikovaného certifikátu verejného kľúča overí, či verejný kľúč na overenie zaručeného elektronického podpisu patrí podpisovateľovi.
(5) Podrobnosti o podmienkach platnosti pre zaručený elektronický podpis, postup pri overovaní a podmienky overenia zaručeného elektronického podpisu ustanoví všeobecne záväzný právny predpis, ktorý vydá úrad.

[7]

Na koľko sa celosvetovo obchodné procesy stále viac digitalizujú, vznikajú neustále rastúce požiadavky na komunikačnú a dátovú bezpečnosť.

Pri použití kvalifikovaného elektronického podpisu môžu byť popri rešpektovaní zákonných ustanovení zmluvne relevantné, časovo kritické a s dôkaznou povinnosťou

transakcie chránené a dokumentované lepšie ako doteraz. Okrem toho sa môžu vytvárať postupy a transakcie pre špeciálne právne záväzne použitie.

Cieľ použitia kvalifikovaných elektronických podpisov je uchovanie integrity a autentity prenášaných dát cez rôzne použitia/platformy ako aj ich nezmeniteľná interpretácia.

Použitie elektronických podpisov napr. : ako alternatíva ručných podpisov popr. Náhrada ručných podpisov je dôležitý element elektronického spracovania dát s právne záväzným charakterom. Zmätky v ´médiách- doteraz spôsobené vytlačením podpísaných dokumentov – sa odbúrajú použitím elektronických podpisov.

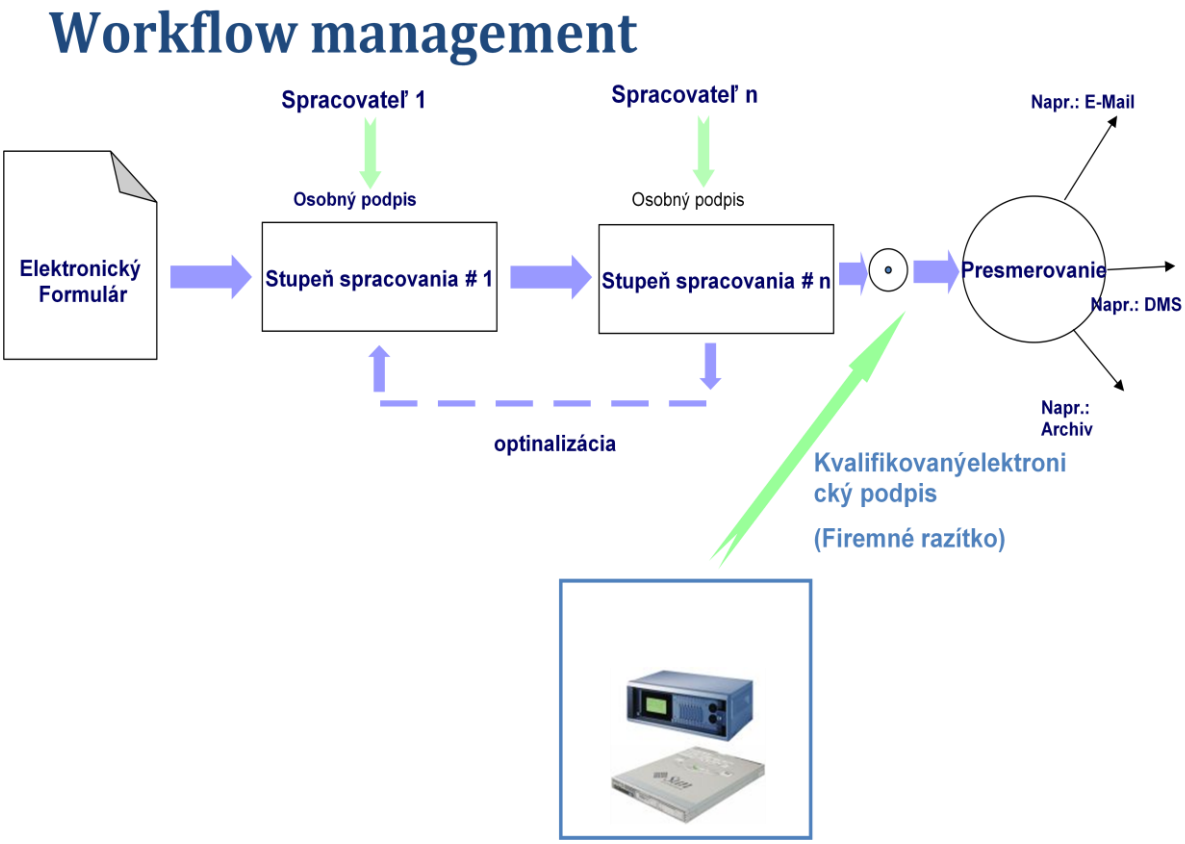
Používaný Hash-Algoritmus (napr.: SHA1) vypočíta jednoznačnú hodnotu pre predložený dokument. Táto hodnota predstavuje ako keby „odtlačok prsta“ dokumentu.

Kvalifikované podpisy je možné zhotoviť výlučne s čipovými kartami/SmartCards.

Na týchto kartách sú uložené:

- certifikát vlastníka
- súkromný podpisový kľúč vlastníka
- verejný kľúč certifikačného miesta(Trust-Center).

Tieto karty vydáva výlučne Trust-Center.



Obr. č.1 Workflow management

Elektronický podpis nám ponúka adekvátne zabezpečenie, hlavne nášho know how, čo je nie len pre firmy ale aj pre jednotlivca to najcennejšie

10 BEZPEČNOSTNÍ PRACOVNÍCI

Pre organizáciu je veľmi dôležité, aby boli aj pracovníci dobre zaškolení a v niektorých prípadoch aj preverení národným bezpečnostným úradom. Je dobré mať vykonanú bezpečnostnú expertízu či previerku národného bezpečnostného úradu, no keď zamestnanci, nie sú oboznámený či zaškolený vo vykonávaní svojich povinností a oprávnení, sa všetka snaha zo strany organizácie neguje a je bezpredmetná.

Väčšinou v štátnych podnikoch, kde sa pracuje s informáciami, ktoré majú nejaký stupeň utajenia požiada vedúci úrad o vykonanie bezpečnostnej previerky podľa vyhlášky 331 Národného bezpečnostného úradu z 10. mája 2004 o personálnej bezpečnosti a o skúške bezpečnostného zamestnanca.

10.1 Postup pri určovaní osoby oboznamovať sa s utajovanými skutočnosťami

(1) Pri vykonávaní bezpečnostnej previerky I. stupňa pre stupeň utajenia Vyhradené vedúci vyhodnotí predložené podkladové materiály. Po podpísaní vyhodnotenia vedúcim oboznámi vedúci navrhovanú osobu s povinnosťami pri ochrane utajovaných skutočností a s možnými dôsledkami za ich porušenie, zabezpečí podpísanie záznamu o určení navrhovanej osoby oboznamovať sa s utajovanými skutočnosťami a vyhlásenia o mlčanlivosti. Záznam o určení navrhovanej osoby a vyhlásenie o mlčanlivosti sa prikladajú k dokumentu, ktorým vznikol alebo sa zmenil pracovnoprávny vzťah alebo obdobný pracovný vzťah.

(2) Ak má byť navrhovaná osoba určená na oboznamovanie sa s utajovanými skutočnosťami stupňa utajenia Prísne tajné, Tajné alebo Dôverné, požiada vedúci úrad o vykonanie bezpečnostnej previerky. K žiadosti pripojí podkladové materiály a vyhodnotenie podkladových materiálov. Doplnkovú časť bezpečnostného dotazníka vypĺňa len navrhovaná osoba, ktorá má byť určená na oboznamovanie sa s utajovanými skutočnosťami stupňa utajenia Prísne tajné alebo Tajné.

(3) Po prijatí písomného oznámenia o vydaní osvedčenia vedúci oboznámi navrhovanú osobu s povinnosťami pri ochrane utajovaných skutočností a s možnými

dôsledkami za ich porušenie a zabezpečí podpísanie záznamu o určení navrhovanej osoby oboznamovať

sa s utajovanými skutočnosťami a vyhlásenia o mlčanlivosti.

(4) Písomné oznámenie o výsledku bezpečnostnej previerky, záznam o určení navrhovanej osoby oboznamovať sa s utajovanými skutočnosťami a vyhlásenie o mlčanlivosti sa prikladajú k dokumentu, ktorým vznikol alebo sa zmenil pracovnoprávny vzťah alebo obdobný pracovný vzťah.

(5) V prípade zmeny pracovnoprávneho vzťahu alebo obdobného pracovného vzťahu môže vedúci požiadať úrad o overenie platnosti osvedčenia.

(6) Na vydanie nového osvedčenia sa vzťahujú odseky 2 až 5.

(7) Ak sa oprávnenej osobe zmení rozsah oboznamovania sa s utajovanými skutočnosťami, vedúci vyhotoví záznam o určení navrhovanej osoby oboznamovať sa s utajovanými skutočnosťami so zmeneným rozsahom. Kópia záznamu o určení sa zasiela úradu do 30 dní od vyhotovenia len pri utajovaných skutočnostiach stupňa utajenia Prísne tajné, Tajné alebo Dôverné.

[6]

10.2 Bezpečnostní pracovníci v PKB

V organizáciách priemyslu komerčnej bezpečnosti sú na zamestnancov fyzickej ochrany alebo pátrania zákonom 473/2005 Z.z. dané kritériá, ktoré musia spĺňať. Môže to byť len osoba, ktorá:

a) dosiahla vek 19 rokov,
b) je spôsobilá na právne úkony v plnom rozsahu,
c) je bezúhonná,
d) je spoľahlivá,
e) je zdravotne spôsobilá,
f) je držiteľom preukazu odbornej spôsobilosti.

K týmto kritériám je veľmi podstatné, aby bezpečnostní zamestnanci vedeli ako sa majú správať počas bežnej prevádzky organizácie, kde vykonávajú fyzickú ochranu, v krízových

situáciách a samozrejme čo zahŕňa nutná obrana, zadržanie a obmedzenie osobnej slobody podozrivej osoby v prípade narušenia objektu kriminálnymi živlami.

- **Nutná obrana:**

- Čin inak trestný, ktorým niekto odvracia priamo hroziaci alebo trvajúci útok na záujem chránený týmto zákonom, nie je trestným činom. (Zákon č. 300/2005 Z.z.).
- Nejde o nutnú obranu, ak obrana bola celkom zjavne neprimeraná útoku, najmä k jeho spôsobu, miestu a času, okolnostiam vzťahujúcim sa k osobe útočníka alebo k osobe obrancu.
- Ten, kto odvracia útok spôsobom uvedeným v odseku 2, nebude trestne zodpovedný, ak konal v silnom rozrušení spôsobenom útokom, najmä v dôsledku zmätku, strachu alebo zľaknutia.
- Ak sa niekto vzhľadom na okolnosti prípadu mylne domnieva, že útok hrozí, nevylučuje to trestnú zodpovednosť za čin spáchaný z nedbanlivosti, ak omyl spočíva v nedbanlivosti.

- **Obmedzenie osobnej slobody podozrivej osoby:**
  Osobnú slobodu osoby, ktorá bola pristihnutá pri trestnom čine alebo bezprostredne po ňom, smie obmedziť ktokoľvek, ak je to potrebné na zistenie jej totožnosti, na zabránenie úteku alebo zaistenie dôkazov. Je však povinný túto osobu odovzdať ihneď vyšetrovateľovi alebo policajnému orgánu, príslušníka ozbrojených síl môže odovzdať aj najbližšiemu útvaru ozbrojených síl alebo správcovi posádky. Ak takú osobu nemožno ihneď odovzdať , treba niektorému z uvedených orgánov obmedzenie osobnej slobody bez odkladu oznámiť. Ak takú osobu prevzal iný orgán ako vyšetrovateľ, je povinný ju ihneď odovzdať vyšetrovateľovi.

V mnohým prípadoch je jednoduchšie zamestnancom vysvetliť tieto pojmy na príklade ako ich zaťažovať zákonným výkladom. Môžeme názorne vysvetliť na prípade, v ktorom páchateľ kameňom rozbije výkladnú skriňu obchodu:

- Poškodený príde napríklad na miesto činu v čase, keď páchateľ už hádže kameň, a nemôže mu v tom zabrániť. V takom prípade útok páchateľa už fakticky skončil a poškodený nemôže konať v rámci nutnej obrany. Keďže páchateľa pristihol pri trestnom čine alebo bezprostredne po ňom, môže postupovať podľa trestného

poriadku a obmedziť ho na osobnej slobode fyzickým zadržaním. Takéto zadržanie možno realizovať rôznymi spôsobmi – fyzickým prekonaním odporu páchateľa, zamknutím páchateľa do bytu, pivnice, skladu a pod., spútaním páchateľa, hrozbou, že bude použitá zbraň, ak sa pokúsi o útek, a pod. Nie je pravda, že na obmedzenie osobnej slobody podozrivého páchateľa je oprávnená len polícia alebo iný orgán činný v trestnom konaní. Obmedziť slobodu podozrivého pristihnutému pri trestnom čine alebo bezprostredne po ňom môže ktokoľvek, nie len orgán štátu alebo poškodený, ale aj náhodná osoba.

- Okrem obmedzenia osobnej slobody podozrivého páchateľa sa zasahujúca osoba po prekonaní odporu útočníka môže určite presvedčiť, či nemá pri sebe zbraň, vziať mu na určitý čas osobné doklady a zistiť jeho totožnosť alebo iné veci, ktoré sú dôležité ako dôkaz.
- Nutná obrana a obmedzenie osobnej slobody podľa trestného poriadku môžu prebiehať súčasne. Ak by napadnutý bojoval s útočníkom a bránil by mu hodiť kameň do drahej výkladnej skrine, postupoval by predovšetkým podľa ustanovenia § 25 Trestného zákona o nutnej obrane, čo je určite výhodnejšie ako podľa trestného poriadku. Ak by ho v rámci takého súboja izoloval a obmedzil na osobnej slobode, obmedzenie osobnej slobody by bolo súčasťou postupu podľa § 25 Trestného zákona, čo je pre zasahujúceho podstatne výhodnejšie.
- Počas obmedzenia osobnej slobody podozrivého a do jeho odovzdania policajnému orgánu nesmie zasahujúci, nech už by sa cítil akokoľvek poškodený, páchateľa trestať.

[8]

II. PRAKTICKÁ ČÁST

Praktická časť bola vykonávaná na reálnom objekte, nachádzajúci sa v Novom Meste nad Váhom s názvom IMV Industry s.r.o. Bezpečnostný projekt bol spracovaný v súčinnosti s bezpečnostným koordinátorom organizácie.

11 ANALÝZA RIZÍK

11.1 Miera bezpečnostných rizík

Úroveň bezpečnostných rizík bola stanovená tak ako je uvedené v nasledovnej tabuľke :

BR	Názov	Miera rizika
1.	Zlyhanie mechanických zábranných prostriedkov (MZP)	Stredná
2.	Zlyhanie technických zabezpečovacích prostriedkov (TZP)	Stredná
3.	Neúmyselné poškodenie MZP a TZP – neodborná manipulácia	Stredná
4.	Narušenie chráneného priestoru úmyselné – vlámaním	Stredná
5.	Odcudzenie US oprávnenou osobou cudzou	Malá
6.	Odcudzenie US neoprávnenou osobou cudzou	Malá
7.	Neúmyselné poškodenie US – neodborná manipulácia	Malá
8.	Vyzradenie US	Malá
9.	Zneužitie US „treťou stranou“ (návštevy, servis, a pod.)	Malá
10.	Poškodenie nosičov informácií v číslicovej forme (MD, CD),	Stredná
11.	Úmyselná zmena obsahu informácií v číslicovej forme (MD, CD),	Malá
12.	Poškodenie dokumentov v dôsledku zlyhania prostriedkov OFB	Stredná
13.	Znehodnotenie dokumentov v dôsledku zlyhania prostriedkov OFB	Stredná
14.	Zničenie dokumentov v dôsledku zlyhania prostriedkov OFB	Stredná
15.	Únik informácií s US v odpade (neplatné dokumenty alebo médiá)	Malá
16.	Zemetrasenie	Malá
17.	Technologické havárie (plyn, voda, elektrina)	Stredná

Tabuľka č.2 Bezpečnostné riziká

Celková miera rizika vychádza ako **STREDNÁ.**

11.2 Hrozby

Konkrétne, pre daný chránený priestor (CHP) sú aktuálne nasledovné ***hrozby***:

- živelná pohroma (požiar, víchrica, zemetrasenie, blesk s následkom požiaru),
- technologické havárie (výbuch plynu, porucha elektrického rozvodu),
- katastrofy,
- úmyselné narušenie objektu a chránených priestorov (vlámanie, teroristický útok),
- sabotáž s cieľom získať prístup k IT (vyradenie zdroja elektrickej energie s cieľom vyradiť z činnosti EZS, úmyselne založený požiar, vyradenie EZS).

12 BEZPEČNOSTNÝ PLÁN OCHRANY OBJEKTU A CHRÁNENÉHO PRIESTORU

12.1 Umiestnenie a opis objektu

Spoločnosť IMV Industry s.r.o. sa nachádza na ulici Bavlnárska 52 v Novom Meste nad Váhom. V objekte sa nachádza jednopodlažná budova a má samostatný vchod z parkoviska pred budovou kde sa nachádza hlavná vrátnica.

Ide o jednopodlažnú administratívne - prevádzkovú budovu. Pozemok je obdĺžnikového tvaru. Budova je prefabrikovaná betónová skeletová budova obložená prefabrikovanými výplňami. (hrúbka stien 300 mm).

12.2 Ochrana objektu

Hranica objektu je zabezpečená mechanickými zábrannými prostriedkami. Celý pozemok je ohraničený betónovými platňami do výšky 1,8 m a ukončené ostnatým drôtom. Hlavný vchod budovy je opatrený kovovými dverami so zámkom, ktorý je trvalo kontrolovaný strážnou službou.

12.3 Chránený priestor

Je zabezpečený mechanickými zábrannými prostriedkami t. j. vchod do chráneného priestoru je zabezpečený bezpečnostnými dverami značky ADLO BD 200 T2 so 4 bodovým uzamykacím mechanizmom, zárubňou zaliatou betónom a ukotvenou do konštrukcie múru, ktorého hrúbka je 300 mm. Okná chráneného priestoru sú drevené osadené v kovových rámoch o rozmeroch 1500 x 1000 mm, ktoré sa dajú otvoriť a neotvárateľnými presklenými časťami o rozmeroch 1000 x 300 mm. Výška okna nad úrovňou terénu je cca. 15 m. Mechanické zábranné prostriedky podľa certifikátov zodpovedajú bezpečnostnej triede a ide o :

Názov MZP	Popis výrobku	Výrobca	Číslo certifikátu	Držiteľ certifikátu	Kategória certifikátu	Platnosť certifikátu
Bezpečnostné Dvere a zárubne	Adlo BD 200T2	Adlo bezpečnostné dvere s.r.o.	T 11-0171/2003	Adlo bezpečnostné dvere s.r.o.	„T“	11.11. 2010
Zámkový mechanizmus	MUL T LOCK	Rostex Vyškov, s.r.o.	T 10-0628/2004	Rostex Vyškov, s.r.o.	„T“	19.06. 2012
Cylindrická vložka	MUL T LOCK	MUL-T-LOCK Ltd. Izrael	T 10-0284/2003	D-Marketing Slovakia, s.r.o.	„T“	09.05. 2014
Úschovný objekt	YETY KK	Spell SB, s.r.o. Prešov	T 09-0077/2003	Spell SB, s.r.o. Prešov	„T“	01.08. 2006
Zámkový mechanizmus	Typu „B“	MAUER	T 09-0077/2003	Spell SB, s.r.o. Prešov	„T“	20.04. 20013

Tabuľka č.3 MZP

Chránený priestor je zabezpečený technickými zabezpečovacími prostriedkami v súlade s STN 334590, 334590-1 až 8. Na vchodových dverách je umiestnený prístupový systém ovládaný bezkontaktnou proximity kartou a magnetickým kontaktom. Vnútorné priestory chráneného priestoru sú zabezpečené priestorovými detektormi, detektormi na rozbitie skla, magnetickými detektormi na vchodových dverách a oknách, špeciálnym tiesňovým hlásičom. EZS objektu, ale je samostatne ovládaný LCD klávesnicou s prepojením na prístupový systém. Technické zabezpečovacie prostriedky zodpovedajú bezpečnostnej triede a ide o :

Názov TZP	Popis výrobku	Výrobca	Číslo certifikátu	Držiteľ certifikátu	Kategória certifikátu	Platnosť certifikátu
Ústredňa EZS	PX - 18	Guardall Limited Škótsko	T 02-0253/2003	Fittich Alarm s.r.o., Banská Bystrica	„PT“	23. 06. 2008
Prístupový systém	PX - 18	Guardall Limited	T 02-0253/2003	Fittich Alarm s.r.o., Banská	„PT“	23. 06.

		Škótsko		Bystrica		2008
RIZ EZS	PX - 18	Guardall Limited Škótsko	T 02-0253/2003	Fittich Alarm s.r.o., Banská Bystrica	„PT“	23. 06. 2008
Priestorový detektor	V 12 AM	Guardall Limited Škótsko	T 02-0281/2003	Fittich Alarm s.r.o., Banská Bystrica	„PT“	08. 07. 2008
Detektor na rozbitie skla	5812A-W	Sentrol Inc. USA	T 02-0168/2003	Fittich Alarm s.r.o., Banská Bystrica	„PT“	14. 04. 2008
Tiesňový hlásič	3045	Sentrol Inc. USA	T 02-0272/2003	Fittich Alarm s.r.o., Banská Bystrica	„PT“	01. 07. 2008
Magnetický detektor	1085 W	SENTROL Inc.	T 02-0167/2003	Fittich Alarm s r.o. Banská Bystrica	„PT“	14. 04. 2008
Magnetický detektor	1078	SENTROL Inc.	T 02-0166/2003	Fittich Alarm, s r.o. Banská Bystrica	„PT“	14. 04. 2008

Tabuľka č.4 TZP

13 REALIZÁCIA BEZPEČNOSTNEJ POLITIKY V OBLASTI FYZICKEJ A OBJEKTOVEJ BEZPEČNOSTI

Realizácia bezpečnostnej politiky v uvedenej oblasti spočíva v zavedení protiopatrení podnikateľa na minimalizovanie bezpečnostných rizík v oblasti fyzickej a objektovej bezpečnosti.

BR	***Protiopatrenie***
zlyhanie mechanických zábranných prostriedkov	Preventívne: technická údržba, servis, kontroly Detekčné: autodiagnostika, vizuálna kontrola Eliminačné: minimalizovanie počtu používaných MZP, jednoduchá konštrukcia
zlyhanie technických zabezpečovacích prostriedkov	Preventívne: pravidelné servisné prehliadky, vytváranie záloh Detekčné: vizuálna kontrola Eliminačné: minimalizovanie počtu používaných TZP
neúmyselné poškodenie MZP a TZP – neodborná manipulácia	Preventívne: pravidelné školenia, preskúšanie, kontrola Detekčné: vizuálna kontrola Eliminačné: vylúčiť z obsluhy MZP a TZP nepreškolených zamestnancov
narušenie chráneného priestoru úmyselné - vlámaním	Preventívne: dodržiavanie režimových opatrení, upratovanie zabezpečiť len oprávnenými osobami Detekčné: detektor pohybu, kamera pred vstupom do CHP Eliminačné: prístupový prostriedok, kódovanie pri vstupe oprávnenou osobou
bezpečnostné riziká prostriedkov OFB vo vzťahu k *informačným technickým prostriedkom :*	
poškodenie nosičov informácií	Preventívne: používanie kvalitných nosičov

v číslicovej forme (MD, CD),	informácií, zálohovanie Detekčné: nefunkčnosť MD, CD Eliminačné: minimalizovanie počtu nosičov informácií
úmyselná zmena obsahu informácií v číslicovej forme (MD, CD),	Preventívne: prístupové práva, udržovanie dobrých vzťahov na pracovisku, monitorovanie nežiaducich vzťahov oprávnených osôb Detekčné: zmena obsahu informácií Eliminačné: minimalizovanie počtu oprávnených osôb a vstupov do CHP
bezpečnostné riziká prostriedkov OFB vo vzťahu k *administratívnym prostriedkom*	
poškodenie dokumentov v dôsledku zlyhania prostriedkov OFB	Preventívne: servis, kontroly MZP a TZP, preskúšavanie obsluhy Detekčné: zlyhanie prostriedkov OFB Eliminačné: minimalizovanie počtov prostriedkov OFB, jednoduchosť a účelnosť systémov technického a fyzického zabezpečovania OUS
znehodnotenie dokumentov v dôsledku zlyhania prostriedkov OFB	Preventívne: servis, kontroly MZP a TZP, preskúšavanie obsluhy Detekčné: zlyhanie prostriedkov OFB Eliminačné: minimalizovanie počtov prostriedkov OFB, jednoduchosť a účelnosť systémov technického a fyzického zabezpečovania OUS
zničenie dokumentov v dôsledku zlyhania prostriedkov OFB	Preventívne: servis, kontroly MZP a TZP, preskúšavanie obsluhy Detekčné: zlyhanie prostriedkov OFB Eliminačné: minimalizovanie počtov prostriedkov OFB, jednoduchosť a účelnosť systémov technického a fyzického zabezpečovania OUS
únik informácií v odpade (neplatné dokumenty alebo médiá)	Preventívne: používanie skartovačky na ničenie neplatných dokumentov a médií

	Detekčné: kontrola realizovania opatrení, vykonávaná vedúcim Eliminačné: kontrola osôb pri opustení CHP
bezpečnostné riziká spojené s *krízou* (mimoriadna udalosť, mimoriadna situácia, vojna)	
zemetrasenie	Preventívne: dôsledné dodržiavanie požiarnych predpisov v celom objekte Detekčné: zmyslovo (receptory) Eliminačné: zákaz používania otvoreného ohňa a fajčenia v CHP, hasiaci prístroj
technologické havárie (plyn, voda, elektrina)	Preventívne: pravidelné revízie rozvodov plynu, vody a elektrických vedení, znalosť o dislokácii hlavných uzáverov, nácviky technologických havárií podľa spracovaných plánov Detekčné: technologická havária – zmyslovo (receptory) Eliminačné: dodržiavanie termínov revízií, udržiavanie návykov osôb v CHP

Tabuľka č.5 Protiopatrenia fyzickej a objektovej bezpečnosti

13.1 Elektrický zabezpečovací systém a systém kontroly vstupov

Elektrický zabezpečovací systém v uvedenom prípade sa navrhuje riešiť ako súčasť už existujúceho elektrického zabezpečovacieho systému (EZS) a to pomocou priestorovej, plášťovej ochrany, predmetovej ochrany, ochrany osôb a protisabotážnej ochrany. K vyhodnocovaniu stavov EZS sa navrhuje použiť riadiace a indikačné zariadenie PX - 18, v ktorom je implementovaný aj systém SKV (systém kontroly vstupov), ktorým sa bude riadiť režim vstupu do chráneného priestoru.

Priestorová ochrana sa navrhuje vykonať pomocou priestorového detektora.

Plášťová ochrana sa navrhuje vykonať pomocou magnetických detektorov vo vstupných dverách, na oknách v miestnostiach a detektoroch rozbitia skla.

Ochrana osôb sa navrhuje vykonať pomocou špeciálneho tiesňového hlásiča na ovládanie rukou, ktorý sa navrhuje umiestniť vedľa vstupných dverí.

Pred vstupom do objektu sa navrhuje umiestniť externá proximity čítačka bezkontaktných kariet a klávesnice prostredníctvom ktorej sa bude vykonávať identifikácia osoby vstupujúcej do chráneného priestoru.

Riadiace a indikačné zariadenie je umiestnené v miestnosti č.101 na 1 poschodí spolu s pripojovacím modulom systému SKV, doplnkovým zdrojom a komunikačným modemom pripojeným na hlavnú vrátnicu..

Ovládanie systému v chránenom priestore sa bude vykonávať samostatne a nezávisle na EZS v objekte a to pomocou jedného ovládacieho panela, ktorý sa navrhuje umiestniť vedľa vstupu do miestnosti.

Vyvedenie poplachového signálu sa navrhuje realizovať pomocou metalického prepojenia na hlavnú vrátnicu.

13.2 Technický popis zariadení EZS

13.2.1 Riadiace a indikačné zariadenie PX - 18

Riadiace a indikačné zariadenie PX 18 patrí k najnovšiemu radu vyhodnocovacích zariadení firmy Guardall. Riadiace a indikačné zariadenie a celý zabezpečovací systém umožňuje inštaláciu a programovanie tak, aby boli splnené požiadavky vysokej bezpečnosti a spoľahlivosti, jednoduchosti inštalácie, obsluhy a cenovej dostupnosti. Jeho modulová koncepcia umožňuje maximálne využitie komponentov systému. Dáva k dispozícii nezávislé ovládanie 4 zón - skupiny detektorov, ktoré môžu pracovať samostatne. Dvadsať možných užívateľov, dáva možnosť prideliť každému obsluhujúcemu svoj vlastný kód s príslušnou právomocou. Má osemnásť vstupov a pamäť päťsto udalostí.

Možnosť kontrolovať prístup k jednotlivým skupinám pomocou LCD klávesníc, proximity čítačiek.

Riadiace a indikačné zariadenie (RIZ) môže byť ovládané nasledovnými spôsobmi:

a) Pomocou ovládacích panelov s dvojriadkovým displejom a klávesnicou, pričom na RIZ môže byť pripojených štyri ovládacie panely.

b) RIZ môže byť ovládané pomocou ovládacieho panela s „proximity čítačkou“.

Riadiace a indikačné zariadenie má napäťovo nezávislú vnútornú pamäť, kde sa zaznamenávajú jednotlivé stavy zariadenia, (kto, ako a kedy zapol alebo vypol systém či zónu, kedy a kde bol poplach, kedy a kto programoval systém a pod.). Kapacita uvedenej pamäte je 500 stavov.

Riadiace zariadenie má potencionálové, alebo bezpotencionálové výstupy na ovládanie akustických, optických a komunikačných zariadení. Ďalej je možné jej rozšírenie o ďalšie dosky reléových výstupov, vnútorného komunikátora, monitorovania akumulátora a pod.

RIZ umožňuje pripojiť na dosku desať zabezpečovacích slučiek. Ďalšie rozšírenie systému je dané počtom použitých klasických koncentrátorov. Pre PX - 18 to môžu byť najviac dva koncentrátory, kde maximálny celkový počet zabezpečovacích slučiek je 18.

Celý systém je napájaný jednosmerným napätím 12V. Toto sa získava zo sieťového stabilizovaného napájacieho zdroja 1 A. V prípade potreby sa k tomuto zdroju pridá vonkajší zdroj - akumulátor, ktorým je pri výpadku siete zálohovaný celý systém. Pri bežnej prevádzke je akumulátor automaticky dobíjaný zo sieťového zdroja.

Obr. č.2 Zariadenia PX-18

13.2.2 Ovládací panel

Ovládací panel sa používa na ovládanie systému poverenými pracovníkmi. Obsahuje LCD displey 2 x 16 znakov a 15 tlačidlovú klávesnicu. Ovládací panel sa používa v dialógovom režime s obsluhou k riadeniu všetkých funkcií systému. Umožňuje čítať údaje o každom stave, okamihy narušenia, zapnutie a vypnutie systému, oprávnenosť vstupu do systému. Ovládací panel je umiestnený na chodbe pred vstupom do chráneného priestoru.

Ovládací panel s riadiacim a indikačným zariadením vyžaduje prepojenie štvoržilovým tieneným káblom. Napájacie napätie je 12V =, odber 10 mA.

13.2.3 Ďalšie použité prvky:

- priestorový detektor Guardall V 12 AM
- magnetický detektor Sentrol 1078
- magnetické detektory Sentrol 1085
- tiesňový hlásič na ovládanie rukou Sentrol 3045

- detektor rozbitia skla Sentrol 5812 A-W

- doplnkový zdroj DZN 12V/3A s akumulátorom 17 Ah

Riadiace a indikačné zariadenie je potrebné napojiť z hlavného rozvádzača objektu zo samostatného okruhu. Z toho dôvodu je potrebné zabezpečiť silnoprúdový prívod pre RIZ káblom CYKY 3Cx1,5 mm^2 v zmysle STN 33 4590 čl. 5.2., istič v rozvádzači označiť „ EZS- nevypínať “ a káblom SYKFY 5x2x0,5 prepojiť na rozvod JTS. Pre vzájomné prepojenie prvkov EZS navrhujeme použiť káble SYKFY uložené v elektroinštalačných PVC žľaboch., lištách na povrchu.

13.2.4 Zoznam certifikovaných MZP a TZP

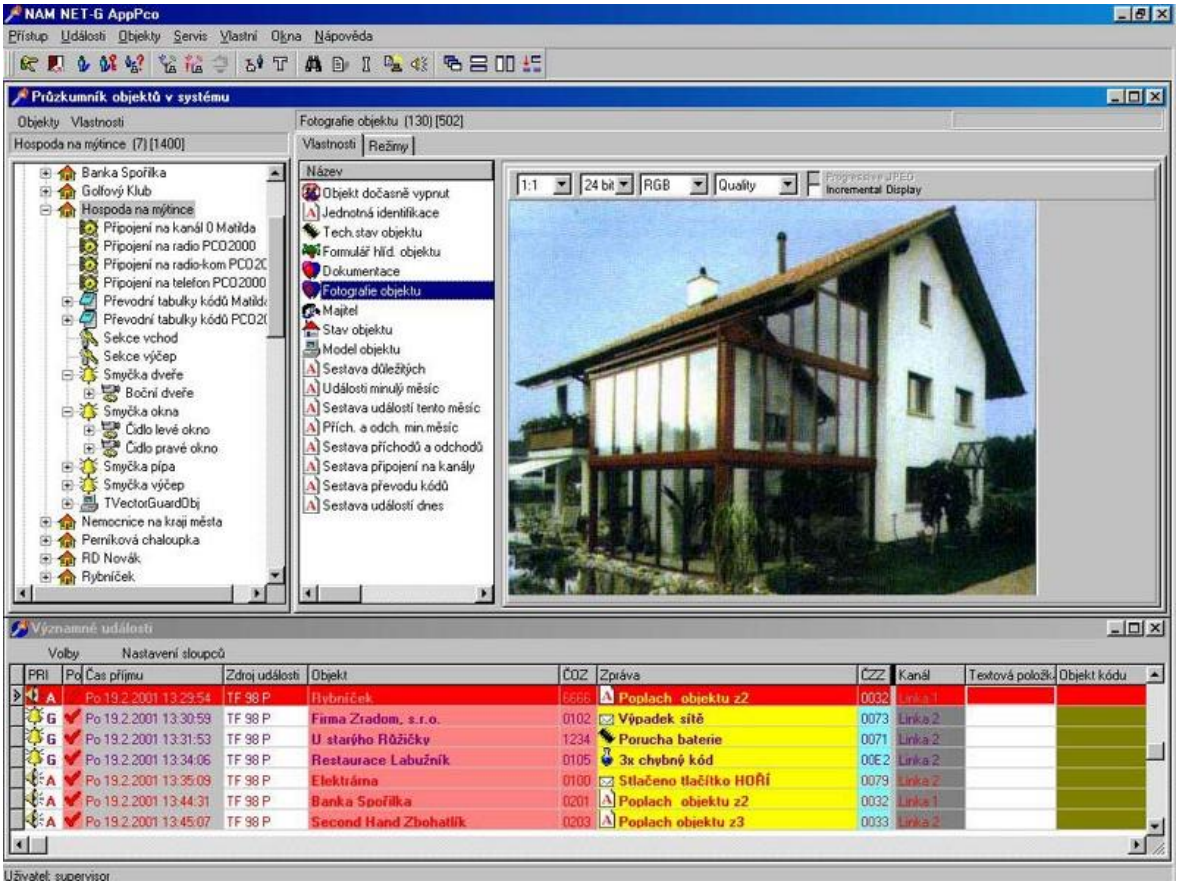
Názov MZP	**Popis výrobku**	**Výrobca**	**Číslo certifikátu**	**Držiteľ certifikátu**	**Kategória certifikátu**	**Platnosť certifikátu**
Bezpečnostné dvere a zárubne	ADLO BD200T2	ADLO Bezpečnostné dvere s.r.o.	T 11-0171/2003	ADLO Bezpečnostné dvere, s.r.o. Bratislava	„T“	23.04. 2013
Zámkový mechanizmus	MUL-T-LOCK	Rostex Vyškov, s.r.o.	T 10-0628/2004	Rostex Vyškov, s.r.o.	„T“	29.06. 2014
Cylindrická vložka	MUL-T-LOCK	MUL-T-LOCK Ltd., Izrael	T 10-0284/2003	D-MARKETING SLOVAKIA, s.r.o., Žilina	„T“	08.07. 2015
Úschovný objekt	YETY KK	Spell SB, s.r.o. Prešov	T 09-0077/2003	Spell SB, s.r.o. Prešov	„T“	26.02. 2014

Tabuľka č. 6 Certifikované MZP

Názov TZP	Popis výrobku	Výrobca	Číslo certifikátu	Držiteľ certifikátu	Kategória certifikátu	Platnosť certifikátu
Ústredňa EZS	PX - 18	Guardall Limited Škótsko	T 02-0253/2003	Fittich Alarm s.r.o., Banská Bystrica	„PT“	23. 06. 2014
RIZ EZS	PX - 18	Guardall Limited Škótsko	T 02-0253/2003	Fittich Alarm s.r.o., Banská Bystrica	„PT“	23. 06. 2015
Prístupový systém	PX - 18	Guardall Limited Škótsko	T 02-0253/2003	Fittich Alarm s.r.o., Banská Bystrica	„PT“	23. 06. 2015
Priestorový detektor	V 12 AM	Guardall Limited Škótsko	T 02-0281/2003	Fittich Alarm s.r.o., Banská Bystrica	„PT“	08. 07. 2015
Detektor na rozbitie skla	5812A-W	Sentrol Inc. USA	T 02-0168/2003	Fittich Alarm s.r.o., Banská Bystrica	„PT“	14. 04. 2014
Tiesňový hlásič	3045	Sentrol Inc. USA	T 02-0272/2003	Fittich Alarm s.r.o., Banská Bystrica	„PT“	01. 07. 2012
Magnetický detektor	1085 W	SENTROL Inc.	T 02-0167/2003	Fittich Alarm s r.o. Banská Bystrica	„PT“	14. 04. 2013
Magnetický detektor	1078	SENTROL Inc.	T 02-0166/2003	Fittich Alarm, s r.o. Banská Bystrica	„PT“	14. 04. 2013
Skartovací stroj	IDEAL 2250 CC	Krug & Priester GmbH & Co. KG	T 06-0433/2003	Utax Slovakia, s.r.o.	„D“	22.10. 2014

Tabuľka č. 7 Certifikované TZP

Všetky prvky systému EZS sú certifikované Národným bezpečnostným úradom. Katalógové listy jednotlivých zariadení sú k dispozícii u bezpečnostného pracovníka podnikateľa.



Obr. č. 3 EZS

Obr. č. 4 EPS

13.3 Časový plán realizácie, materiálne a finančné nároky na jej zabezpečenie

Protiopatrenia, uvedené v časti 13 projektu budú realizované podľa časového plánu, materiálne a finančné nároky na zabezpečenie objektovej a fyzickej bezpečnosti sú uvedené v nasledujúcich tabuľkách

Časový plán realizácie			
Názov prostriedku		Realizácia	
		Od	Do
MZP		*d.d. m. m. rrrr*	*d.d. m. m. rrrr*
	Stavebné úpravy	22.4.2011	10.08.2011
	Bezpečnostné dvere a zárubne - osadenie	22.4.2011	10.08.2011
	Úschovný objekt – upevnenie	22.4.2011	10.08.2011
	Skartovacie zariadenie - nákup - umiestnenie	22.4.2011	10.08.2011
TZP			
	Projektová dokumentácia	08.4.2011	10.08.2011
	Dodávka zariadení EZS+SKV	22.4.2011	10.08.2011
	Dodávka elektroinštalačného materiálu	22.4.2011	10.08.2011
	Montážne práce zariadení EZS+SKV a EPS	15.4.2011	10.08.2011
	Elektroinštalačné práce	05.4.2011	10.08.2011

Tabuľka č. 8 Časový plán realizácie

Náklady na realizáciu		
Názov prostriedku		**Náklady;EURO**
MZP		
	Bezpečnostné dvere a zárubne	1500.- EUR
	Zámkový mechanizmus uzamykací	
	Cylindrická vložka	
	Úschovný objekt (trezor)	900.- EUR
	Skartovacie zariadenie	500.- EUR
	Náklady celkom s DPH (MZP)	**2900.- EUR**
TZP		
A1 :	Dodávka zariadení EZS+SKV	1185,20 EUR
A2 :	Dodávka elektroinštalačného materiálu	148,80 EUR
B1 :	Montážne práce zariadení EZS+SKV	985,80 EUR
B2 :	Elektroinštalačné práce	687.- EUR
C :	Projektová dokumentácia	136.- EUR
	Spolu A1+A2+B1+B2+C bez DPH	3142,80 EUR
	DPH 20% z A1+A2+B1+B2+C	628,56 EUR
	Náklady celkom s DPH (TZP)	**3771,6.- EUR**
	Náklady celkom s DPH :	**6671,6,- EUR**

Tabuľka č. 9 Náklady na realizáciu

14 KRÍZOVÝ PLÁN OCHRANY OBJEKTU

14.1 Režimové opatrenia

Poplachový signál z objektu a chráneného priestoru je vyvedený na hlavnú vrátnicu spoločnosti. V prípade zaznamenania poplachového signálu pracovníkmi hlavnej vrátnice títo vyrozumejú určených pracovníkov spoločnosti a následne Policajný zbor. Určení pracovníci poskytnú zásahovej skupine policajného zboru účinnú spoluprácu, umožnia vstup do objektu a vykonanie prehliadky objektu. Určený pracovník okamžite vyrozumie o udalosti vedúceho objektu. Po vykonaní ohliadky a potrebných úkonov príslušníkmi zásahovej skupiny Policajného zboru, vykoná preskúšanie a zapnutie EZS pod ochranu a následne uzamkne objekt.

V prípade mimoriadnej situácie (živelná pohroma, havária, požiar, katastrofa a pod.) sú zamestnanci spoločnosti IMV povinní :

Uzavrieť hlavý uzáver plynu a vody a odpojiť hlavný prívod elektrickej energie.

Nahlásiť uvedenú skutočnosť na príslušný útvar:

policajného zboru	tel. 158, 112
mestskej polície	tel. 159
požiarneho zboru	tel. 150, 112
lekárska záchranná služba	tel. 155, 112
plynárne	tel. 7716356
vodárne	tel. 6520592
elektrárne	tel. 0850 111555

Všetky režimové opatrenia sú podrobne rozpísané systéme ochrany.

14.2 Kontrola režimových opatrení

Kontrolu aktuálnosti dokumentácie, poučenie zodpovedných osôb, postup pri mimoriadnej situácii, pri narušení objektu a reakčného času fyzickej ochrany na poplachový signál vykonáva najmenej raz ročne generálny riaditeľ a bezpečnostný zamestnanec. Uvedené skutočnosti vyznačí v knihe kontrol.

15 ZABEZPEČENIE INFORMAČNÝCH TECHNOLÓGIÍ

15.1 Možné riziká ohrozenia informačných technológií

Z hľadiska používania informačných technológií by vo všeobecnosti bezpečnostným rizikom mohli byť samotné technické a systémové prostriedky. Konkrétne ich zlyhanie, znehodnotenie alebo poškodenie. Ďalšou skupinou rizík je únik, zneužitie alebo zámerná modifikácia informácií. Samostatnú skupinu rizík tvoria riziká plynúce z krízového stavu (výpadky energie, poruchy hardvéru a softvéru, živelná pohroma, požiar, povodeň a pod.). Ďalej porušenie predpisov a smerníc osobami, nedostatky v kontrolnej činnosti bezpečnostného správcu, správcu informačného systému, vedúceho a ďalších.

Rozsah bezpečnostných rizík bude minimalizovaný použitím certifikovanej autonómnej pracovnej stanice (technickým prostriedkom bude samostatne pracujúci počítač), umiestnený v chránenom priestore a minimalizovaním výstupov v podobe utajovaných dokumentov.

Z uvedených všeobecných bezpečnostných rizík pre spoločnosť IMV vyplývajú v oblasti informačnej bezpečnosti ako významné tieto bezpečnostné riziká:

- bezpečnostné riziká vyplývajúce z neexistencie riadenia prístupu k objektom a službám technického prostriedku

- bezpečnostné riziká vyplývajúce z nejednoznačnej identifikácie a autentizácie používateľa

- bezpečnostné riziká vyplývajúce z nemožnosti nastaviť voliteľné riadenie prístupu k objektom technického prostriedku a jeho službám na základe rozlišovania a správy prístupových práv používateľa, jeho identity alebo členstva v skupine používateľov

- bezpečnostné riziká vyplývajúce z nevytvárania kontrolného záznamu technických prostriedkov o svojej činnosti

- bezpečnostné riziká vyplývajúce z nedostatočne podrobného kontrolného záznamu technických prostriedkov o svojej činnosti

- bezpečnostné riziká vyplývajúce z absencie monitorovania (kontroly) kontrolného záznamu o činnosti technického prostriedku

- bezpečnostné riziká vyplývajúce z neodstránenia utajovaných skutočností, ktoré nie sú potrebné na ďalšie spracovanie, archiváciu alebo manipuláciu (operačná pamäť, dočasné súbory a pracovné súbory)

- bezpečnostné riziká vyplývajúce zo zlyhania technického prostriedku alebo jeho časti

- bezpečnostné riziká vyplývajúce zo zemetrasenia, požiaru, povodne

- bezpečnostné riziká vyplývajúce zo zlyhania ľudského faktora oprávnených osôb

15.2 Technický prostriedok

Technickým prostriedkom je samostatná PC stanica bez pripojenia na internú alebo externú počítačovú sieť. Pracovná stanica je vybavená malou disketovou mechanikou na vytváranie záloh používateľských dátových súborov pre potreby zabezpečenia havarijného plánovania a obnovy činnosti technického prostriedku a mechanikou CD/CD-RW/DVD-HL-DT-ST GCC4480B pre potreby iniciálnej inštalácie systémových prostriedkov a pre potreby zabezpečenia havarijného plánovania a obnovy činnosti technického prostriedku, ako aj vytváranie záloh používateľských dátových súborov s utajovanými skutočnosťami. K vytváraniu záloh používať len značkové CD/DVD zapisovateľné (Recordable) nosiče.

PC stanica sa nachádza v priestore, kde majú povolený vstup len oprávnené osoby s odpovedajúcim určením pre prácu. Dokumenty (výstupy z tlačiarne a zálohy súborov pre potreby zabezpečenia havarijného plánovania a obnovy činnosti technického prostriedku)

budú zaevidované, ukladané a prepravované v súlade systémových opatrení. Používané administratívne pomôcky sú zaevidované v Knihe administratívnych pomôcok.

15.2.1 Schválenie technického prostriedku do prevádzky

Technický prostriedok bude schválený do prevádzky (*Protokol o schválení technického prostriedku do prevádzky)* vedúcim podnikateľa po dodaní certifikovaného technického prostriedku od dodávateľa. Vedúci zabezpečí vypracovanie *Protokolu o schválení technického prostriedku do prevádzky*.

15.2.2 Organizačné opatrenia a systém kontroly

Po nákupe certifikovaného technického prostriedku „samostatne pracujúci počítač“ vykoná správca informačného systému inštaláciu MS Office a antivírusového prostriedku. Potom bezpečnostný správca a správca informačného systému zriadia používateľov pracovnej stanice a pracovná stanica je pripravená do prevádzky o čom vedúci vystaví protokol..

Vedúci vykonáva *nepravidelné* (neočakávané) *kontroly* a *pravidelné* (plánované) kontroly v oblasti informačnej bezpečnosti. Cieľom kontrol je zistenie skutočného stavu plnenia povinností správcu pracovnej stanice a používateľov pracovnej stanice.

16 PERSONÁLNE ZABEZPEČENIE OCHRANY

16.1 Možné riziká ohrozenia z hľadiska personálnej bezpečnosti

Možné hrozby je možné obecne charakterizovať ako zlyhanie ľudského faktoru vo vzťahu k sebe samému, k iným osobám (fyzickým, právnickým), technickým prostriedkom (informačným, mechanickým zábranným, technickým zabezpečovacím) a administratívnym prostriedkom.

V spoločnosti IMV bude potrebné minimalizovať nasledovné personálne bezpečnostné riziká

Riziko	Protiopatrenie
vznik poruchy správania sa oprávnených osôb	Prevencia : *neformálny kontakt, monitorovanie práce* Eliminácia *: zrušenie oprávnenia a určenia osoby*
zmena bezúhonnosti oprávnených osôb	Prevencia : *neformálny kontakt, monitorovanie práce* Eliminácia *: zrušenie oprávnenia a určenia osoby*
porušenie mlčanlivosti osôb	Prevencia : *neformálny kontakt, monitorovanie práce* Eliminácia *: zrušenie oprávnenia a určenia osoby*
rizikové vzťahy k iným osobám (bezpečnostne nespoľahlivým),	Prevencia : *neformálny kontakt, monitorovanie práce* Eliminácia *: zrušenie oprávnenia a určenia osoby*
znižovanie odbornej spôsobilosti oprávnených osôb,	Prevencia : *školenie, precvičovanie* Eliminácia *: preskúšanie*
neadekvátne vysoký počet oprávnených osôb,	Prevencia : *prehodnocovanie organizovania práce* Eliminácia *: optimalizácia počtu*
prístup „tretích strán“ (návštevy)	Prevencia :*minimalizovanie návštev* Eliminácia *: zrušenie návštev*

Tabuľka č. 10 Protiopatrenie pri personálnej bezpečnosti

17 SYSTÉM OCHRANY

1. Úvod.

Strážnu službu je možné chápať ako sústavu vzájomne súvisiacich preventívnych opatrení administratívneho a výkonného charakteru, pomocou ktorých má byť zaistená ochrana majetku, bezpečnosť života a zdravia zamestnancov a osôb nachádzajúcich sa v chránenom objekte. Objektom sa rozumie komplex budov a priestorov na ktoré sa vzťahuje tento systém ochrany.

Prevenciu definujeme ako množinu všetkých aktivít smerujúcich k predchádzaniu bezpečnostných rizík a páchania trestných a iných protispoločenských činov, k znižovaniu ich výskytu cestou zamedzenia a neutralizácie príčin a podmienok ich vzniku. Činnosť súkromnej bezpečnostnej služby (ďalej len SBS) je zameraná hlavne na prevenciu situačnú, ktorá má za cieľ minimalizovať kriminogénne podmienky v konkrétnej dobe, na konkrétnom mieste a za konkrétnych okolností.

Ochrana majetku (ďalej len ochrana) sa realizuje systémom interných bezpečnostných predpisov, preventívnych opatrení za využitia špeciálnych techník (elektrická zabezpečovacia signalizácia na hlásenie narušenia – EZS, elektrická požiarna signalizácia – EPS, kamerové systémy a pod.) a hlavne fyzickou ochranou zamestnancami SBS.

2. Popis objektu.

a) Adresa : IMV Industry, s.r.o., Nové Mesto nad Váhom (plán objektu príloha č. 2).
b) Miesta so zvýšeným bezpečnostným rizikom.
   - Určené priestory zabezpečené inštalovanou EZS.
c) Miesta so zvýšeným požiarnym rizikom.
   - Určené priestory zabezpečené inštalovanými požiarnymi hlásičmi.

3. Zodpovednosť za ochranu.

a) Ochranu riadi poverený vedúci zamestnanec SBS Trenčín, s.r.o., (ďalej len SBS), ktorý zodpovedá za jej komplexné zabezpečenie, úroveň a vykonávanie v súlade s príslušnými predpismi.
b) Za vytvorenie podmienok pre zodpovedajúcu ochranu, zodpovedajú poverení zamestnanci objednávateľa.

c) Za výkon ochrany zodpovedá vedúci strediska SBS zabezpečujúcej ochranu daného objektu.

4. Rozsah ochrany.

SBS ako vykonávateľ, zabezpečuje ochranu ak sa jedná o majetok :

a) Objednávateľa,
b) V inom vlastníctve a objednávateľ zodpovedá za vzniknutú škodu na tomto majetku.

5. Technické opatrenia k ochrane

5.3. Mechanické zábranné prostriedky.

a) Pozemky, prípadne územne súvisiace pozemky v správe či užívaní objednávateľa musia byť na svojej hranici chránené zodpovedajúcim oplotením, pokiaľ hranicou pozemku objednávateľa nie je budova v jeho správe. Druh oplotenia musí byť zvolený tak, aby oplotenie výrazne sťažovalo prístup do objektu jeho prekonaním.
b) Stav oplotenia musí byť pravidelne, minimálne raz do týždňa kontrolovaný z hľadiska plnenia jeho ochrannej funkcie. Pri zistení poškodenia oplotenia musí byť závada čo v najkratšom čase odstránená. Za technický stav oplotenia zodpovedá objednávateľ a za kontrolu stavu oplotenia zodpovedá SBS. To isté platí aj pre vonkajšie osvetlenie v objekte.
c) Vstupy a vjazdy na oplotené pozemky v správe či užívaní objednávateľa, musia byť opatrené pevnými zabudovanými bránami alebo bránkami, ktoré sa musia dať uzavrieť a uzamknúť.
d) Vstupy do budov a východy z budov objednávateľa musia byť vybavené pevnými dverami alebo bránami, ktoré sa dajú uzavrieť a uzamknúť.
e) Okná budov objednávateľa sa musia dať uzavrieť tak, aby ich nebolo možné otvoriť zvonka. Prípadné vetracie otvory musia byť vybudované tak, aby neumožňovali, pokiaľ sú ponechané otvorené, neoprávnený vstup do budovy.
f) Pomocné zariadenia, napr.: kotolne, garáže, príručné skladové priestory, sa musia dať uzavrieť a uzamknúť.
g) Mrežami musia byť vybavené okná do miestností so zvýšeným bezpečnostným rizikom (napr. pokladne, kde sa nachádzajú utajované skutočnosti a pod.).

h) Trezormi musia byť vybavené miestnosti kde sa pracuje s finančnou hotovosťou a obdobnými hodnotami, drahými kovmi, utajovanými skutočnosťami a pod.

i) Po skončení pracovnej zmeny musia byť kancelárie, sklady, vchody a východy z budov a na pozemky objednávateľa, pokiaľ v nich už nikto nepracuje, uzamknuté a kľúče od nich uložené na mieste na to určenom, riadne označené o akú miestnosť ide. Ďalej musia byť uzavreté všetky okná s výnimkou vetracích okienok, ktoré nie sú jednoduchým spôsobom dostupné alebo sú vybavené zariadením, ktoré znemožňuje vstup do budovy ich prostredníctvom.

5.2. Elektrická zabezpečovacia signalizácia.

a) EZS inštalovaný:
   - Výstup signálu na osobnej vrátnici.

b) EPS inštalovaná:
   - Výstup signálu na osobnej vrátnici (ústredňa EPS).

6. Režimové opatrenia k ochrane.

6.1. Preukazy povoľujúce vstup/vjazd do chráneného objektu.

Poverený útvar objednávateľa zabezpečuje vlastným zamestnancom, nájomníkom a ich zamestnancom, ktorí majú svoje prevádzky v objekte objednávateľa, resp. iným oprávneným osobám a motorovým vozidlám vlastným a nájomníkov:

a) Preukazy, ktoré ich oprávňujú k vstupu/vjazdu do chráneného objektu objednávateľa,

b) Dočasné preukazy osobám/vozidlám, ktoré dočasne (časovo obmedzene) vstupujú do objektu objednávateľa za účelom plnenia si svojich pracovných povinností pre objednávateľa, resp. nájomníkov. Dočasné preukazy je možno nahradiť menným zoznamom príslušných osôb, resp. vozidiel, ktorý poverený útvar objednávateľa odovzdá na príslušné pevné stanovište strážnej služby,

6..2 Vstup osôb.

Vstup do objektu objednávateľa vchodmi určenými k tomuto účelu je povolený :

a) Zamestnancom objednávateľa, resp. nájomníkom po predložení platného preukazu.

b) Iným osobám, po predložení platného dočasného preukazu, poprípade na základe vypracovaného zoznamu, pokiaľ vstupujú do časti, v ktorej plnia úlohy vyplývajúce z ich pracovnej činnosti.
c) Osobám určeným vedením organizácie objednávateľa (určené interným oznámením).
d) Osobám za účelom návštevy po ohlásení a odsúhlasení navštíveným zamestnancom, ktorý si návštevu osobne preberie v priestore vrátnice a zodpovedá za jej pohyb po areáli.
e) Príslušníkom Policajného zboru SR (ďalej len PZ SR), príslušníkom Hasičského a záchranného zboru (ďalej len HaZZ), pokiaľ účelom ich vstupu je činnosť vyplývajúca z ich funkcie v sprievode zodpovednej osoby objednávateľa.
f) Zamestnancom zdravotníckej služby, pokiaľ účelom vstupu je poskytnutie prvej pomoci alebo odvoz chorej osoby v sprievode zodpovednej osoby objednávateľa.
g) Zamestnancom plynárenskej, vodárenskej resp. elektrorozvodnej služby po predložení ich preukazu totožnosti, pokiaľ účelom vstupu je odstránenie poruchy v sprievode zodpovednej osoby objednávateľa.
h) Identifikácia osôb uvedených v odstavci e) až g) sa nevyžaduje, pokiaľ je potrebný rýchly a bezodkladný zásah.
i) Vstup maloletých osôb je možný len v sprievode dospelej osoby, ktorá zodpovedá za jeho pohyb v objekte.
j) Obmedzenie vstupu:
   - Vstup osôb, ktoré sú zjavne pod vplyvom alkoholických nápojov, resp. omamných prostriedkov je prísne zakázaný,

6.3. Výstup osôb.

Výstup z objektu objednávateľa je povolený tými východmi, ktorými je povolený vstup.

Návštevy majú povolený výstup z objektu miestom, ktorým vstúpili do objektu.

Strážna služba neskúma dôvod odchodu osôb z objektu.

6.4. Vjazd vozidiel.

Cestné komunikácie v objekte musia mať riadne dopravné značenie s dôrazom na parkovacie miesta pre motorové vozidlá, ktoré parkujú v objekte.

K vjazdu cestných vozidiel slúži vrátnica. Vjazd je povolený vozidlám :

a) Ktoré majú vydaný preukaz umožňujúci vstup do chráneného objektu.
b) Zabezpečujúcim dodávky pre alebo od objednávateľa, resp. nájomníkom sídliacim v objekte.
c) Rýchlej zdravotníckej pomoci, PZ SR, HaZZ, plynárenskej, vodárenskej a elektrorozvodnej služby v prípade **nutného zásahu.**
d) Obmedzenie vjazdu:
   - Vozidlám, ktoré nezabezpečujú dodávky pre objednávateľa, resp. nájomníkom sídliacich v objekte. Výnimku povoľuje vedenie objednávateľa.
   - Dodávateľským vozidlám v mimopracovnú dobu, ak nie je zabezpečené vyloženie nákladu.
   - Vozidlám, ktorých vodiči sú zjavne pod vplyvom alkoholických nápojov, resp. omamných prostriedkov je vjazd prísne zakázaný.

6.5. Výjazd vozidiel.

Výjazd osobných motorových vozidiel je povolený bránou, ktorou vozidlo do objektu prišlo. Nákladné motorové vozidlá majú povolený výjazd aj bránou určenou len pre tieto vozidlá, pokiaľ nedošlo k ich uzavretiu.

6.6. Kľúčový režim.

Objednávateľ určí, ktoré kľúče podliehajú evidencii a úschove na určenom pevnom stanovišti strážnej služby. Tieto kľúče musia byť riadne označené o akú miestnosť ide a uložené v zapečatenej schránke. Objednávateľ vypracuje menný zoznam osôb (s ich vzorovými podpismi), ktoré môžu tieto kľúče preberať. Zamestnanci SBS vedú príslušnú evidenciu o vydávaní a preberaní určených kľúčov.

6.7. Režimové opatrenia – kontrola

Osoby vstupujúce, vystupujúce, resp. vozidlá vchádzajúce, vychádzajúce do/z objektu podliehajú kontrole zamestnancami SBS v zmysle zákona č. 473/2005 Z.z. v znení neskorších predpisov.

6.8. Režim vrátnice.

Vrátnica slúži na vstup, výstup osôb a vjazd, výjazd vozidiel z/do objektu.

Strážna služba zabezpečuje:

- plnenia režimu vstupu a výstupu osôb v zmysle bodov 6.2. a 6.3.,
- evidenciu návštev,
- poskytovanie kvalifikovaných informácií návštevníkom objektu v potrebnom rozsahu,
- vydávanie a preberanie určených kľúčov a vedenie príslušnej evidencie,
- ohlasovňu požiarov,
- plnenia režimu vjazdu a výjazdu motorových vozidiel v zmysle bodov 6.4. a 6.5.,
- evidenciu prichádzajúcich a odchádzajúcich vozidiel ,
- sledovanie obrazu na monitore poskytovaného kamerovým systémom so zameraním na porušovanie stanoveného systému ochrany,
- pochôdzkovú činnosť v zmysle vypracovaného plánu obchádzok,
- počas pochôdzkovej činnosti je brána vrátnice zatvorená.

6.9. Režimové opatrenia – priestory špeciálneho určenia.

Jedná sa o priestory (resp. objekty), ktoré sú určené na ukladanie alebo manipuláciu s utajovanými skutočnosťami. Ochrana týchto priestorov sa zabezpečuje v zmysle bezpečnostného štandardu fyzickej bezpečnosti a objektovej bezpečnosti vypracovaného pre objednávateľa v zmysle vyhlášky Národného bezpečnostného úradu.

7. Časový rozsah výkonu ochrany.

Z hľadiska časového sa jedná o strážnu službu nepretržitú, vykonávanú zamestnancami SBS.

8. Stanovištia zamestnancov SBS.

Zamestnanci SBS vykonávajú strážnu službu na pevných a pohyblivých stanovištiach. Tieto stanovištia sú určené charakterom objektu objednávateľa.

8.1. Pevné stanovište – umiestnenie:

- Vrátnica – nachádza pri hlavnom vstupe do chráneného objektu.

8.2. Pochôdzková činnosť:

Vykonáva sa podľa vypracovaného plánu obchádzok.

9. Organizácia SBS.

a) Zamestnanci SBS sú organizovaní v stredisku SBS. Vedúceho strediska príslušného objektu ustanovuje do funkcie a odvoláva z funkcie konateľ SBS. V určených prípadoch určuje vedúci so súhlasom konateľa svojho zástupcu a vedúcich zmien.

b) Zamestnancom SBS môže byť len osoba staršia ako 19 rokov, ktorá je telesne, duševne a odborne spôsobilá na výkon fyzickej ochrany podľa ustanovení zákona č. 473/2005 Z.z. v znení neskorších predpisov

9.1. Výstroj a výzbroj zamestnancov SBS.

a) Zamestnancom SBS pre výkon fyzickej ochrany prináleží rovnošata s označením SBS a identifikačným preukazom pripevneným na ľavom prsnom vrecku rovnošaty.

b) Pri výkone fyzickej ochrany na určených miestach patria zamestnancom SBS vecné bezpečnostné prostriedky podľa povahy chráneného objektu (ako sú: obušok, slzotvorný plyn, putá, krátka strelná zbraň, pes).

9.2. Povinnosti vedúceho strediska SBS.

Riadi a organizuje výkon strážnej služby objektu objednávateľa zamestnancami SBS.

K tomuto účelu hlavne:

a) Riadi a organizuje plnenie úloh v oblasti fyzickej ochrany stanovených právnymi predpismi, týmto systémom ochrany a iniciatívne navrhuje nadriadenému opatrenia ku skvalitneniu výkonu strážnej služby.

b) Zabezpečuje materiálne podmienky pre činnosť strediska SBS.

c) Rozpracovaním rozvrhu služieb stanoví rozdelenie zamestnancov SBS na jednotlivé stanovištia, operatívne rieši zabezpečenie strážnej služby v prípade nenastúpenia alebo predčasného ukončenia služby zamestnanca SBS.

d) Kontroluje výkon strážnej služby vrátane pripravenosti zamestnancov SBS k výkonu fyzickej ochrany, hlavne s dôrazom na znalosť vydaných smerníc a pokynov.
e) Operatívne vykonáva príslušné opatrenia k mimoriadnym udalostiam a bezodkladne informuje povereného zamestnanca objednávateľa a svojho nadriadeného o vykonaných opatreniach.
f) Vedie resp. kontroluje denný záznam o priebehu výkonu strážnej služby.
g) Pravidelne kontroluje funkčnosť mechanických zábranných prostriedkov a zabezpečovacej techniky.
h) Dbá o riadne ustrojenie a upravenosť zamestnancov SBS a ich slušné vystupovanie voči okoliu.
i) Podáva návrhy na disciplinárne opatrenia svojmu priamemu nadriadenému.
j) Pripravuje mesačné hlásenie o výkone strážnej služby daného objektu.
k) Denne predkladá poverenému zamestnancovi objednávateľa knihu hlásenia strážnej služby k podpisu, za účelom odstraňovania zistených nedostatkov.

9.3. Vedúci strediska SBS je nadriadený zamestnancom strediska SBS a podriadených priamo riadi

10. Povinnosti zamestnancov SBS

10.1. Zamestnanci SBS sú pri výkone fyzickej ochrany na určenom stanovišti povinní hlavne:

a) Strážiť majetok a s využitím svojich oprávnení zabrániť jeho rozkrádaniu, strate, zneužitiu, poškodeniu a zničeniu.
b) Zabrániť neoprávnenému vstupu osôb alebo neoprávnenému vjazdu dopravných prostriedkov do priestorov objednávateľa.
c) Kontrolovať s využitím svojich oprávnení osoby a dopravné prostriedky, ktoré opúšťajú priestor objednávateľa, predovšetkým za účelom zistenia, či nie je neoprávnene vynášaný alebo vyvážaný majetok, ktorého ochranu vykonávajú.
d) Plniť úlohy vyplývajúce z predpisov o ochrane pred požiarmi (OPP) objednávateľa.
e) Nepodávať žiadne informácie o svojich spolupracovníkoch a pracovnom režime na stanovištiach.

f) Dodržiavať povinnosť mlčanlivosti vymedzenú zákonom č. 473/2005 Z.z. v znení neskorších predpisov

g) Spolupracovať s orgánom štátneho dozoru pri kontrole výkonu ochrany a o kontrole ihneď informovať svojho nadriadeného.

10.2. <u>Zamestnanci SBS sú ďalej povinní:</u>

a) Nastúpiť k výkonu ochrany včas a vykonať písomné prevzatie služby zápisom do knihy služieb a pri ukončení jej písomné odovzdanie nastupujúcemu zamestnancovi SBS.

b) Operatívne s využitím svojich oprávnení vykonávať opatrenia k splneniu povinností uvedených v bode 10.1.

c) Zaznamenávať do knihy hlásenia strážnej služby všetky udalosti vybočujúce z rámca systému ochrany, hlavne so zameraním na popis mimoriadnych udalostí a taktiež do formuláru „Protokol udalosti“.

d) Dôsledne preverovať oprávnenia k vstupu do objektu, u vstupujúcich, ktorí nemajú oprávnenie vstupu dôsledne overovať ich totožnosť a umožniť vstup len v prípadoch stanovených týmto systémom ochrany.

e) Pri vjazde vozidiel do objektu objednávateľa zapisovať vozidlá do knihy evidencie odchodov a príchodov vozidiel (zápis údajov podľa predtlače).

f) V období mimo stanovenú pracovnú dobu, hlavne v dňoch pracovného pokoja, zabrániť vstupu do objektu objednávateľa zamestnancom objednávateľa, pokiaľ im v túto dobu nie je vstup zvlášť povolený. To isté platí aj pre vjazd motorových vozidiel.

g) Poznať zabezpečovacie zariadenia (EZS) a jeho obsluhu, po prijatí signálu z takéhoto zariadenia preveriť príčinu a zariadiť príslušné opatrenia.

h) Vstúpiť do uzavretého priestoru (napr.: kancelárie, sklady atď.) len v prípade zabránenia vzniku mimoriadnej udalosti.

i) Bezodkladne oznamovať poverenému zamestnancovi objednávateľa (a v prípade prečinu, resp. trestného činu aj príslušným orgánom PZ SR) :

- Zistené prípady neoprávneného vstupu osoby alebo vjazdu vozidla, pokiaľ sa tomu nepodarilo zabrániť.
- Neoprávnené vynášanie alebo vyvážanie majetku objednávateľa.
- Iné udalosti, u ktorých je podozrenie z porušovania systému ochrany, ktoré boli pri výkone strážnej služby zistené.

j) Pri kontrole osôb a ich batožiny dbať na česť, vážnosť a dôstojnosť kontrolovanej osoby, ako i svoju vlastnú.

k) Prísne dodržiavať prevádzkové predpisy pri práci s rádiostanicou a mobilným telefónom.

l) Po prijatí signálu civilnej ochrany bezodkladne vykonať príslušné opatrenia podľa smerníc objednávateľa.

10.3. Povinnosti zamestnancov SBS v oblasti OPP.

a) V zmysle zákonných ustanovení sú zamestnanci SBS v záujme OPP povinní:
   - Zúčastňovať sa školenia o OPP v určenom rozsahu.
   - Pri vykonávaní ochrany orientovať pozornosť na priechodnosť prístupových a zásahových miest k objektom a zariadeniam požiarnej ochrany.
   - Sledovať vznik dymu, unikanie pary a poškodzovanie zariadení požiarnej ochrany.
   - Bezodkladne likvidovať vzniknutý požiar, ak to nie je možné okamžite urobiť, vyhlásiť požiarny poplach v zmysle požiarno poplachových smerníc objednávateľa.
   - Bezodkladne oznamovať poverenému zamestnancovi objednávateľa zistené nedostatky, ktoré môžu viesť k vzniku požiaru.
   - Poznať rozmiestnenie hl. uzáverov vody, plynu a el. energie.

b) EPS.

   V prípade prijatia signálu z EPS :
   - Okamžite preveriť hlásený ohrozený priestor.
   - V prípade požiaru tento bezodkladne likvidovať, ak to nie je možné, vyhlásiť požiarny poplach.
   - Zaevidovať v dokumentácii EPS a knihe hlásenia strážnej služby príslušné údaje.

10.4. Oprávnenia zamestnancov SBS.

Zamestnanec SBS je oprávnený zamedziť ďalšej jazde vozidiel :

a) Vodič vozidla v správe objednávateľa nepredloží ku kontrole platný príkaz k jazde alebo vyváža majetok objednávateľa, ktorého vyvezenie nie je uvedené v príslušných dokladoch predložených ku kontrole.

b) Do objektu vchádza vozidlo inej organizácie, ktorého vodič a spolujazdci nemôžu preukázať stanoveným spôsobom svoju totožnosť alebo účel vjazdu.

c) Preukázateľne nie je zabezpečené vyloženie nákladu privezeného vozidlom inej organizácie.

d) Vozidlo inej organizácie vyváža majetok objednávateľa, ktorého vyvezenie nie je povolené v príslušných dokladoch predložených pri kontrole a nie je preukázané oprávnenie vodiča disponovať s týmto majetkom.

e) Vodič vchádzajúceho resp. odchádzajúceho vozidla je zjavne pod vplyvom požitých alkoholických nápojov resp. omamných prostriedkov.

f) Vozidlo vchádza alebo odchádza v dobe, keď je vjazd a výjazd zakázaný. Toto ustanovenie sa nevzťahuje na vozidlá uvedené v bode 6.4.b) v čase nutného zásahu.

g) Vozidlo vchádza alebo odchádza miestom, ktoré nie je k tomuto účelu určené.

Zamestnanci SBS sú ďalej oprávnení:

h) Kontrolovať osoby, ktoré vstupujú do objektu alebo ho opúšťajú, ich batožinu a požadovať predloženie príslušných dokladov.

i) Požadovať v objekte od každého potrebné vysvetlenie pri podozrení z poškodzovania majetku.

j) Vyzvať v objekte každého, kto ohrozuje život alebo zdravie iného alebo majetok, aby od tohto konania upustil.

k) Predviesť na určené miesto každého, kto:
   - Nemôže hodnoverne preukázať svoju totožnosť.
   - Spôsobí poškodenie na zdraví alebo smrť iného, alebo škodu na majetku.
   - Neuposlúchne výzvu podľa ustanovenia písmena j).

l) Odňať vec, ak je dôvodné podozrenie, že bola odcudzená z majetku objednávateľa.

m) Presvedčiť sa či predvádzaná osoba nie je ozbrojená, a v prípade nálezu zbrane túto odobrať.

n) Použiť vecné bezpečnostné prostriedky a to na odvrátenie útoku na seba alebo inú osobu, na prekonanie odporu, ktorý smeruje k zmareniu plnenia jeho úloh, ako aj k zabráneniu úteku predvádzanej osoby.

10.5. Osobitné oprávnenia zamestnancov SBS.

Zamestnanec SBS je oprávnený prehliadať osoby vstupujúce resp. odchádzajúce z objektu objednávateľa. Prehliadku môže vykonať len osoba rovnakého pohlavia a vo vyhradenom priestore v prípadoch:

a) Ak má dôvodné podozrenie, že je neoprávnene vynášaný majetok, ktorého ochranu vykonáva alebo sú neoprávnene donášané veci s cieľom ich v objekte objednávateľa opraviť, upraviť a pod.
b) Ak má dôvodné podozrenie, že sú donášané do objektu objednávateľa alkoholické nápoje.
c) Ak poverený zamestnanec objednávateľa nariadi kontrolnú akciu, prehliadku zamestnancov a osôb vstupujúcich alebo opúšťajúcich objekt objednávateľa.
d) Kontrolovať v celom areáli objednávateľa zákaz fajčenia a dbať na jeho dodržiavanie (v prípade, ak takýto zákaz platí).

Ďalšie osobitné oprávnenia zamestnancov SBS:

e) Použiť úder strelnou zbraňou a výstrahu.
f) Pri ochrane použiť strelnú zbraň ako krajný prostriedok aby:
   - V prípade nutnej obrany odvrátil útok vedený proti jeho osobe alebo mu bezprostredne hroziaci alebo na život inej osoby.
   - Odvrátil nebezpečný útok, ktorý ohrozuje chránený objekt alebo stanovište, po márnej výzve, aby sa od útoku upustilo.
   - Zamedzil úteku nebezpečného páchateľa, ktorého nemôže iným spôsobom zastaviť.
   - Zneškodnil zviera, ktoré ohrozuje život alebo zdravie osôb v chránenom objekte.

10.6. Postup zamestnancov SBS v súvislosti s použitím ich oprávnení.

a) Pri použití oprávnenia uvedeného v bode 10.4. k) je povinný ihneď oznámiť obmedzenie osobnej slobody osoby príslušnému oddeleniu PZ SR a svojmu nadriadenému.
b) Pred použitím vecných bezpečnostných prostriedkov je zamestnanec SBS povinný, ak to okolnosti prípadu dovoľujú, použiť dohováranie, napomenutie alebo výzvu.

c) Pri použití vecných bezpečnostných prostriedkov je zamestnanec SBS povinný použiť len taký prostriedok, ktorý umožňuje splnenie jeho úloh a pritom čo najmenej poškodzuje osobu, proti ktorej sa zakročuje.

d) Pri zákroku proti jednotlivej osobe nesmie zamestnanec SBS použiť vecné bezpečnostné prostriedky, proti tehotnej žene, osobe so zjavnou telesnou chybou, osobe vysokého veku a proti dieťaťu, s výnimkou prípadov, keď to povaha útoku vedeného touto osobou proti chráneným záujmom alebo mimoriadnosť vzniknutej situácie nevyhnutne vyžaduje.

e) Zamestnanec SBS je povinný pred použitím strelnej zbrane, ak to okolnosti prípadu dovoľujú, použiť prostriedky uvedené pod písm. b).

f) Zamestnanec SBS je v súvislosti s použitím strelnej zbrane povinný:

- Dbať na potrebnú opatrnosť, najmä aby nebol ohrozený život iných osôb, a čo najviac šetriť život osoby, proti ktorej použitie strelnej zbrane smeruje.
- Poskytnúť zranenej osobe, len čo to okolnosti prípadu dovolia, prvú pomoc, prípadne zabezpečiť jej lekárske ošetrenie. To isté platí aj pri použití akéhokoľvek oprávnenia a prostriedkov pri ktorom dôjde k zraneniu osoby.
- Bezodkladne oznámiť použitie strelnej zbrane príslušnému oddeleniu PZ SR a svojmu nadriadenému, a zaistiť podklady pre riadne vyšetrenie prípadu.

g) O použití oprávnení a prostriedkov uvedených v tomto systéme ochrany vykoná zamestnanec SBS záznam v knihe hlásenia strážnej služby, knihe evidencie zásahov a spracuje protokol udalosti. Záznam musí obsahovať najmä popis priebehu udalosti, časové údaje, osobné údaje zúčastnených osôb, včítane svedkov a opatrenia vykonané po použití týchto oprávnení a prostriedkov.

11. Evidencia výkonu ochrany.

K evidencii výkonu ochrany slúži :

a) Kniha služieb – (nachádza sa na určenom pevnom stanovišti) vedúci strediska SBS v nej eviduje menný rozpis služieb zamestnancov SBS na príslušný deň s časom zahájenia a ukončenia, určuje čas a varianty pochôdzkovej činnosti. Do tejto knihy zaznamenáva poznatky inšpekčný orgán SBS, resp. poverený zamestnanec objednávateľa. Eviduje sa v nej preberanie a odovzdanie služby výkonu ochrany.

b) Kniha hlásenia strážnej služby – (nachádza sa na každom pevnom stanovišti) do tejto knihy sú chronologicky zaznamenávané zamestnancami SBS všetky, počas výkonu ochrany zistené nedostatky.
c) Kniha evidencia služieb – (nachádza sa na určenom pevnom stanovišti) do tejto knihy zaznamenáva vedúci strediska SBS fyzické obsadenie služieb (§ 19 vyhláška 634/2005 Z.z. v znení neskorších predpisov).
d) Inšpekčná kniha dozoru – (nachádza sa na určenom pevnom stanovišti) do tejto knihy zaznamenáva výsledok kontroly orgán štátneho dozoru (§ 21 vyhláška 634/2005 Z.z. v znení neskorších predpisov).
e) Kniha evidencie zásahov – (nachádza sa na pevnom stanovišti) v tejto knihe sa evidujú všetky vykonané zásahy, pri ktorých boli použité vecné bezpečnostné prostriedky a obmedzenie osobnej slobody s uvedením všetkých údajov potrebných k vyhodnoteniu zásahov (§ 20 vyhláška 634/2005 Z.z. v znení neskorších predpisov).
f) Kniha evidencie odchodov a príchodov vozidiel – (nachádza sa na pevnom stanovišti, ktoré slúži pre vjazd a výjazd vozidiel) do tejto knihy sa zaznamenávajú všetky prejazdy vozidiel s údajmi podľa predtlače.
g) Kniha evidencie kľúčov – (nachádza sa na pevnom stanovišti, kde sa uschovávajú kľúče) do tejto knihy sa zaznamenávajú všetky výdaje a prijatia určených kľúčov.
h) Kniha evidencie návštev – (nachádza sa na pevnom stanovišti, ktoré slúži pre vstup a výstup osôb) do tejto knihy sa zaznamenávajú všetky osoby vstupujúce do objektu za účelom návštevy.
i) Mesačné hlásenie SBS – vystavuje vedúci strediska SBS, kde sumarizuje zistené nedostatky za príslušný mesiac. Takto pripravené hlásenie predkladá poverenému zamestnancovi objednávateľa, ktorý v ňom písomne hodnotí výkon ochrany.

12. Povinnosti objednávateľa a vykonávateľa pri použití zariadení EZS.

12.1 Rozsah ochrany.

Z hľadiska časového sa jedná o ochranu viazanú na mimopracovný čas objednávateľa. Mimopracovný čas je stanovený dobou od aktivovania poplachového systému na hlásenie narušenia do jeho deaktivovania.

SDBS ako vykonávateľ služieb vykonáva ochranu určených priestorov formou dozornej a zásahovej služby nadväzujúcej na signál z elektrickej zabezpečovacej signalizácie na hlásenie narušenia (ďalej len EZS) o narušení objektu.

Objednávateľ zodpovedá za riadne fungovanie EZS na hlásenie narušenia.

a) Dozorná služba.

Dozornú službu zabezpečuje zamestnanec SBS na hlavnej vrátnici objednávateľa ako dozor nad vyčlenenými priestormi objednávateľa, prostredníctvom EZS inštalovanej v priestoroch objednávateľa s výstupom signálu na osobnej vrátnici.

V rámci zásahu je nutné zabezpečiť:

- V prípade ak je signál vyhodnotený ako narušenie chráneného priestoru:
  - Zistiť, či v chránenom priestore skutočne došlo k narušeniu alebo sa jedná o falošný poplach.
  - **V prípade násilného narušenia chráneného priestoru (zistené vizuálnou kontrolou), zabezpečí zvýšenú ochranu narušeného priestoru do príchodu zodpovedného zamestnanca objednávateľa (max. 30 minút od oznámenia) alebo príslušníkov PZ SR.**
  - V súlade s ustanovením Trestného poriadku, obmedziť osobnú slobodu páchateľa narušenia, pokiaľ k narušeniu došlo a pokiaľ sa páchateľ v chránenom priestore zdržuje, poprípade je na úteku v blízkosti narušeného priestoru a je možné mu ešte obmedziť osobnú slobodu.
  - Zaistiť miesto činu s ohľadom na zachovanie kriminalistických stôp.
  - Stotožnenie prípadných svedkov udalosti a odovzdanie týchto informácií príslušníkom PZ SR.
  - Zdokumentovanie zásahu.

12.2 **Technické a režimovo-technické opatrenia k ochrane.**

Mechanické zábranné prostriedky.

a) Vstupy do priestorov chránených EZS musia byť vybavené pevnými dverami alebo bránami, ktoré sa dajú uzavrieť a uzamknúť.
b) Po skončení pracovnej zmeny resp. po ukončení činnosti v chránenom priestore, musia byť uzavreté a uzamknuté všetky vstupy i okná, s výnimkou vetracích okienok, ktoré nie sú jednoduchým spôsobom dostupné a sú vybavené

zariadením, ktoré znemožňuje vstup do priestoru ich prostredníctvom, osobám i vtáctvu.

12.3 **Povinnosti zamestnancov.**

12.3.1 Povinnosti zamestnancov objednávateľa.

Po ukončení pracovnej zmeny resp. po ukončení činnosti v chránenom priestore, zodpovedný zamestnanec objednávateľa prekontroluje (uzatvorenie dvier, okien, vypnutie elektrických spotrebičov a pod.) a uzavrie chránený priestor a aktivuje EZS.

Na základe výzvy pracovníka SBS zodpovedný zamestnanec je povinný dostaviť sa k miestu narušenia do 30 minút.

13. Kontakt na objednávateľa.

Meno	Adresa	MT	

14. Kontakt na vykonávateľa.

Meno	Adresa	MT	
Dispečer			

15. Záverečné ustanovenia.

Tento systém ochrany je záväzný pre všetkých zamestnancov SBS DMT. Systém doplňujú prípadné smernice a pokyny objednávateľa, ktoré zohľadňujú jeho špecifické požiadavky na ochranu objektu.

Organizačné smernice SBS doplňujúce systém ochrany :

- Strelné zbrane používané pri ochrane objektov.

- Starostlivosť o psov používaných pri ochrane objektov.
- Spojovacie prostriedky.
- Taktické zásady postupu pri mimoriadnych udalostiach.

V Trenčíne, dňa

Objednávateľ: Vykonávateľ:

ZÁVĚR

Pojem bezpečnostná expertíza a bezpečnostný projekt už nie je veľkou neznámou ako bolo v minulosti, keď sa fyzická ochrana riešila jedným zamestnancom, ktorý nemal žiadnu odbornosť ani výcvik či vedomosti o spôsobe ochrany a len si tak povediac odsedel na vrátnici svoju zmenu. Mnoho firiem sa v tejto nebezpečnej dobe začalo zverovať radšej odborníkom z priemyslu komerčnej bezpečnosti ako by si tento problém mali riešiť svojpomocne.

Bezpečnostný projekt je veľmi dôležitým kritériom aj pri uzatváraní poistiek a tak mnohé firmy dbajú na správny výber súkromných bezpečnostných firiem, ktoré im tento projekt spracovávajú.

V mojej práci som chcela ukázať postup pri spracovaní bezpečnostného projektu a ktoré hľadiská sú dôležité pri jeho spracovaní.

ZÁVĚR V ANGLIČTINĚ

Concept security expertise and security project is no longer an unknown quantity as in the past, when the physical protection of employees handled by one that has no expertise or training or knowledge on how to protect you and only so to speak, sat in the reception your shift. Many companies in this dangerous time began to prefer to delegate to experts from the commercial security industry as they would be solve this problem themselves.
Security project is a very important criterion for the award and so many insurance companies care for the proper selection of private security companies, which they handled this project.
In my work I wanted to show the procedure for processing a security project and which aspects are important for its processing.

SEZNAM POUŽITÉ LITERATURY

[1] Brabec, František, , vedoucí autorského kolektívu, Bezpečnosť pro firmu, úřad, občana

[2] Laucký, Vladimír, Judr., Technologie komerční bezpečnosti I

[3] Laucký , Vladimír, Judr., Technologie komerční bezpečnosti II

[4] Laucký, Vladimír, JUDr., Řízení technologických procesú v prúmyslu komerční bezpečnosti

[5] Zákon Slovenskej republiky č 215/2004 Z.z o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov

[6] Vyhláška Národného bezpečnostného úradu 331/2004 o personálnej bezpečnosti a o skúške bezpečnostného zamestnanca

[7] Zákon Slovenskej republiky č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov

[8] Fico, Róbert, Nutná obrana

[9] Valouch, Jan, Ing. Ph.D., Projektování integrovaných systémú,

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BR	Bezpečnostné riziko
CD	Dátový nosič
EPS	Elektrická požiarna signalizácia
EZS	Elektrické zabezpečovacie systémy
HaZZ	Hasičského a záchranného zboru
CHP	Chránený priestor
I&HAS	Poplachový zabezpečovací a tiesňový systém
IT	Informačná technológia
MD	Disketa
MZP	Mechanické zábranné prostriedky
NBÚ	Národný bezpečnostný úrad
OFB	Objektová a fyzická bezpečnosť
OPP	Ochrana pred požiarmi
PKB	Priemysel komerčnej bezpečnosti
PT	Prísne tajné
PZ SR	Policajný zbor Slovenskej republiky
RIZ	Riadiace a indikačné zariadenie
SBS	Súkromná bezpečnostná služba
SKV	Systém kontroly vstupov
T	Tajné
TZP	Technické zabezpečovacie prostriedky
US	Utajované skutočnosti
Z.z.	Zbierka zákonov

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: PÔDORYS OBJEKTU IMV INDUSTRY S.R.O.