Projekt zabezpečení budovy supermarketu a perimetru

Peter Marček

Diplomová práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Peter Marček**
Osobní číslo:	**A13408**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Projekt zabezpečení budovy supermarketu a perimetru**
Téma anglicky:	**A Security Project for a Supermarket Building and its Perimeter**

Zásady pro vypracování:

1. **Klasifikujte jednotlivé stupne zabezpečenia objektov a pozemkov vrátane všeobecných definícií.**
2. **Identifikujte jednotlivé druhy rizík a popíšte základné požiadavky na manažment rizika s popísaním bezpečnostných rizík a technických prostriedkov používaných na ochranu objektov.**
3. **Popíšte jednotlivé technológie a spôsoby ich použitia.**
4. **Vypracujte projekt elektronického zabezpečenia objektu a pozemkov v jeho okolí s ohľadom na kvalitu.**
5. **Navrhnite detektory a senzory potrebné k zabezpečeniu objektu a pozemkov.**
6. **Navrhnite technickú časť pre trvalú obsluhu zariadení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **COOPER, F. – GREY, S. – RAYMOND, G. – WALKER, P. 2004. Project Risk Management Guidelines: Manage Risk in Large Projects and Complex Procurements. 1st ed. Chichester, U.K.: Wiley, 2004. ISBN: 0-470-02281-7.**
2. **KORECKÝ, M. – TRKOVSKÝ, V. 2011. Management rizik projektů. Praha: Grada Publishing, 2011. ISBN: 978-80-247-3221-3.**
3. **KŘEČEK, S. a kol. 2006. Příručka zabezpečovací techniky. Blatná: Cricetus, 2006. ISBN: 80-902938-2-4.**
4. **LOVEČEK, T. – NAGY, P. 2008. Bezpečnostné systémy Kamerové bezpečnostné systémy. Žilina: EDIS vydavateľstvo ŽU, 2008. ISBN: 978-80-8070-891-1.**
5. **VALOUCH, Jan. Projektování bezpečnostních systémů. [skriptum]. Zlín: UTB, 2012. ISBN 978-80-7454-230-5.**
6. **STN EN 50130 – 133 Poplachové systémy, bez ISBN.**

Vedoucí diplomové práce: **Ing. Karel Perůtka, Ph.D.**
Ústav řízení procesů

Datum zadání diplomové práce: **12. ledna 2015**

Termín odevzdání diplomové práce: **15. května 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

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 připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- 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/bakalářské 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

ABSTRAKT

Diplomová práca sa zaoberá, na základe prieskumu oblastí jednotlivých stupňov zabezpečenia objektov, pozemkov za použitia dostupných technických prostriedkov na trhu, návrhom elekrického zabezpečenia budovy supermarketu a perimetra za účelom ochrany budovy a pozemkov v jej okolí s ohľadom na kvalitu zabezpečenia.

Klíčová slova: riziko, bezpečnostné riziká, bezpečnostný manažment, riadenie rizika, zabezpečenie budovy a okolia, integrované zabezpečovacie systémy

ABSTRACT

This Master thesis deals with design of an electric security of supermarket building and a perimeter, which are based on an areas research of various levels of securing buildings, by using the technical means that are available in the market. The purpose of this thesis is to protect buildings and grounds in their vicinity with respect to quality assurance.

Keywords: risk, security management, risk management, safety risks, security protections building and perimeter, integration security systems

Motto:

„ Niaká pevnosť nie je taká silná, aby ju peniaze nedobyli.“

Marcus Tullius Cicero

OBSAH

ÚVOD

V súčasnom období rastie počet rizík a zvyšuje sa ich komplexnosť a previazanosť. Pojem bezpečnosť sa stáva čoraz viac frekventovanejším a významnejším. Z každého uhla pohľadu sú spoločnosti ohrozované rôznymi druhmi udalostí, ktoré nesú prvky neurčitosti a neistoty a môžu byť pre spoločnosti zdrojom ohrození, nebezpečenstiev. Vo všeobecnosti ide o kozmické, vojenské, technogénne, sociogénne, prírodné, ekologické, ekonomické, ale aj bezpečnostné riziká. Malé spoločnosti nevedia riešiť a ovplyvniť makroriziká na globálnej, ba ani len nacionálnej úrovni, rovnako ako prírodné riziká. Ak riziko vôbec riešia, väčšinou sa zameriavajú na riadenie miery neistoty a neurčitosti ekonomických rizík. Najviac zanedbávanou oblasťou sú technologické a bezpečnostné riziká.

V súčasnosti zaznamenávame obrovský vzostup množstva informácií na celom svete. „Počítačová revolúcia, znásobenie počtu družíc, šírenie kopírovacích zariadení, videorekordérov, elektronických sietí, databáz, faxov, káblovej televízie, družíc pre priame vysielanie a mnoho ďalších technických zariadení pre spracovávanie a šírenie informácií vytvorilo celé prúdy údajov, informácií a poznania. Tieto zariadenia umožňujú vymieňať si ohromné pakety naplnené akustickým, dátovým a grafickým materiálom, cez nadbytočné a decentralizované kanály. Slovami Tofflera, Tretia vlna zapálila akýsi informačný veľký tresk, keď vytvorila nekonečne sa rozpínajúci vesmír poznania.“ [1]

Rovnako, ako sa informačný tok dá využiť v prospech spoločnosti, tak je aj priamym zdrojom rizík pre spoločnosti. Údaje získané o spoločnostiach, používaných prostriedkoch a technológiách sa často zneužívajú v ich neprospech. V súčasnosti sa vyskytuje ale aj priame využitie technických prostriedkov a zariadení proti spoločnostiam. Takéto riziká spoločnosti musia identifikovať, vyhodnotiť hroziace nebezpečenstvá a prostredníctvom riadenia rizika eliminovať alebo aspoň minimalizovať škody spôsobené neistými udalosťami, ktoré môžu ovplyvniť chod ale aj existenciu podniku. „Obchodné spoločnosti si musia udržať väčšinu zručností a praktík, ktoré sa v minulosti osvedčili. Pokiaľ však dúfajú, že budú v novom prostredí rásť a prosperovať, budú ich musieť doplniť o významné nové kompenzácie a praktiky.“ [2] Takýmito praktikami je aj osvojenie si riadenia rizika a jeho zavedenie do praxe. Význam analýzy a riadenia rizika neustále rastie. Riadenie rizika je kľúčový faktor pre trvalý rast podniku. Bez uvedomenia si hroziacich rizík, vykonania analýzy a vypracovania plánu riešenia rizika je takmer

1 TOFFLER, A. - TOFFLEROVÁ, H. 2002. *Válka a antiválka: Jak porozumět dnešnímu globálnímu chaosu*. s. 177.

2 KOTLER, P. - WONG, V. - SAUNDERS, J. - ARMSTRONG, G.. 2007. *Moderní marketing.* s. 181.

nemožné dosahovať dlhodobý rast spoločnosti, príp. sa vôbec udržať na trhu. Riziko je prevažne spájané s negatívnymi dôsledkami, ale podniky často podstupujú riziko dobrovoľne s cieľom získania pozitívnych výsledkov s využitím naskytujúcej sa príležitosti ako špekulatívne riziko. Riešenie riadenia rizika v podniku je cyklický neustály proces, kde sa po vypracovaní projektu riadenia rizika podniku realizuje stratégia podniku, ktorej súčasťou sú taktiež nadväzujúce manažérske postupy na jej zabezpečenie.

Cieľom diplomovej práce je na základe prieskumu oblastí jednotlivých stupňov zabezpečenia objektov, pozemkov za použitia dostupných technických prostriedkov na trhu navrhnúť projekt elekrického zabezpečenia budovy supermarketu a perimetra za účelom ochrany budovy a pozemkov v jej okolí s ohľadom na kvalitu zabezpečenia.

Prvá kapitola obsahuje teoretické vymedzenie pojmov. Klasifikuje jednotlivé stupne zabezpečenia objektov, identifikuje jednotlivé druhy rizík a popisuje základné požiadavky na manažment rizika s popísaním bezpečnostných rizík a technických prostriedkov používaných na ochranu objektov.

Druhá kapitola je venovaná charakteristike konkrétneho objektu - hypermarketu. Zameriava sa na identifikáciu, analýzu a zhodnotenie jednotlivých rizík a možností manažmentu rizika na riadenie bezpečnostných rizík v podniku. U vybranej skupiny rizík – bezpečnostné riziká - poukazuje na špecifiká pri implementácii v praxi.

Tretia kapitola je analytická časť, ktorá sa venuje implementácii manažmentu rizika v skúmanom podniku so zameraním na bezpečnostný manažment. Bola vykonaná analýza zistených skutočností a tiež bola vytvorená SWOT analýza podniku zo skúmaných dát a z jej výsledku sú vyvodené závery s možným riešením a odporučením k aplikovaniu v praxi za účelom zvýšenia bezpečnosti spoločnosti a zníženia rizík, nebezpečenstiev a možných stavov neurčitosti. Boli použité metódy a techniky na získanie relevantných dát slúžiacich k analýze, ktoré boli východiskom k riešeniu danej problematiky a impulzom pre vykonávanie zberu a skúmaniu dát. V závere je vyhodnotenie práce a rekapitulácia východísk skúmania.

Použité metódy a postupy riešenia: analýza, dedukcia, identifikácia, implementácia, indukcia, klasifikácia, kontrolovanie, meranie, monitorovanie, projektovanie, porovnávanie, syntéza, SWOT, štúdia, triedenie.

Významom riešenia problematiky bolo aplikovať teoretické poznatky, premietnuť na praktické riešenia a následne aplikovať alebo porovnať mieru ich použitia v konkrétnej skúmanej spoločnosti a navrhnúť východiská ich uplatnenia v praxi pri zohľadnení súčasnej legislatívy a STN.

I. TEORETICKÁ ČASŤ

1 TEORETICKÉ ZÁKLADY ZABEZPEČENIA OBJEKTOV

Účelom technického zabezpečenia objektov je zvýšenie bezpečnosti objektu a týmto spôsobom zníženie rizika. Na zvýšenie účinnosti technickej ochrany je vhodné doplnenie systému vhodnými mechanickými zabezpečovacími zariadeniami a režimovými opatreniami, príp. fyzickou ochranou objektu.

1.1 Stupne zabezpečenia objektov a pozemkov

PSN a ich komponenty sú rozdelené do stupňov zabezpečenia podľa požadovanej bezpečnosti. Stupne zabezpečenia sa musia zohľadniť podľa úrovne rizika, ktoré závisí od priestorov, hodnoty majetku v objektoch a predpokladaného typu páchateľa.

PSN musí mať stanovený stupeň zabezpečenia, ktorý bude určovať jeho parametre. Sú určené štyri stupne zabezpečenia, pričom stupeň 1 je základný stupeň a stupeň 4 je najvyšší stupeň. Stupeň zabezpečenia PSN určuje komponent s najnižším stupňom zabezpečenia.

Ak je PSN rozdelený do jasne definovaných podsystémov, potom môže PSN obsahovať komponenty rôznych stupňov v každom systéme. Stupeň podsystému je určený najnižším stupňom komponentu v ňom použitom.

Komponenty, ktoré sú spoločné pre viac podsystémov, musia mať stupeň minimálne rovnaký ako podsystém najvyššieho stupňa.

Ako pomôcka pre zadávateľov, projektantov a osoby zodpovedné za zabezpečenie objektov sú uvedené nasledovné stupne zabezpečenia:

- nízke riziko – predpoklad, že narušitelia majú slabú znalosť o PSN a majú k dispozícii len obmedzený výber ľahko dostupných nástrojov
- nízke až stredné riziko – predpoklad, že narušitelia majú určité znalosti o PSN a použijú aspoň základný sortiment nástrojov a prenosných prístrojov
- stredné až vysoké riziko – predpoklad, že narušitelia sú oboznámení s PSN a majú úplný sortiment nástrojov a elektronických zariadení
- vysoké riziko – používa sa vtedy, ak má zabezpečenie prioritu pred ostatnými hľadiskami. Predpokladá sa, že narušitelia alebo páchatelia sú schopní alebo majú možnosť spracovať podrobný plán vniknutia a majú kompletný sortiment zariadení vrátane prostriedkov na náhradu komponentov PSN.

Pod pojmom narušiteľ sú zahrnuté aj iné ohrozenia – lúpež, hrozba fyzického násilia – ak môžu mať vplyv na návrh systému PSN. [1]

1.2 Definícia, identifikácia a klasifikácia rizík

1.2.1 Definícia rizika

Za historický pôvod termínu riziko sa považujú výrazy:

- RHIZA (grécky) – pomenovanie obavy zo straty nákladu počas plavby,
- RISQ (arabsky) – vyjadrenie obavy z toho, čo nám prinesie narodenie človeka, čo mu bude dané, aby nám prinášalo úžitok,
- RISICUM (latinsky) – výraz používaný v námorníctve na prekonanie nebezpečného útesu, [2]
- RISCO (taliansky) – výraz pre byť v nebezpečenstve. [3]

Definícia rizika nie je presne stanovená a každý autor ju interpretuje inak. Väčšinou ide o nepríjemné skutočnosti alebo javy, hrozby a poškodenia. Vo všeobecnosti ide o narušenie stavu bezpečnosti súvisiace s priamymi alebo následnými stratami a škodami. Napr.

The Oxford Dictionary and Therasaurus uvádza: „Riziko je možnosť nebezpečenstva, straty, zranenia alebo iných škodlivých dôsledkov.“ [4]
Business dictionary: „Riziko je pravdepodobnosť alebo nebezpečenstvo z poškodenia, zranenia, zodpovednosti, straty alebo inej negatívnej udalosti, ktorá je spôsobená vonkajšími alebo vnútornými faktormi, ktoré môžu byť ovplyvňované prostredníctvom preventívnej činnosti.“ [5]

Anglický OGC (Office for Government Commerce - Úrad vlády pre obchod – súčasť ministerstva financií Veľkej Británie) definuje riziko nasledovne: „Neistá udalosť alebo súbor udalostí, ktoré pokiaľ nastanú, budú mať účinok na dosiahnutie cieľov. Riziko sa skladá z kombinácie pravdepodobnosti výskytu vnímanej hrozby alebo príležitosti a veľkosti jej dopadu (impact) na ciele. Hrozba je použitá na popis neistej udalosti, ktorá by mohla mať negatívny dopad na ciele alebo prínosy, príležitosť popisuje neistú udalosť,

1 EN 50 131-1:2006, ICS 13.310, ICS 13.320, STN EN 50 131-1:2007
2 ŠIMÁK, L. 2005. *Manažment rizík. In: Projekt vzdelávania zamestnancov.* s. 81.
3 FARLEX, Inc. 2013. *The free dictionary* [online]
4 OXFORD UNIVERSITY PRESS. 2013. *Oxford dictionaries* [online]
5 WEBFINANCE, Inc. 2013. *Business dictionary* [online]

ktorá by mohla mať priaznivý dopad na ciele alebo prínosy.“[1]

Cooper z iného uhla pohľadu definuje vznik rizika ako dôsledok neistoty ohľadne budúcnosti. [2]

Terminológia krízového riadenia SR: Riziko je potenciálna možnosť narušenia bezpečnosti systému, objektu alebo procesu. Je to pravdepodobnosť vzniku krízového javu a jeho dôsledku.

Smernica EÚ Seveso II: Riziko je pravdepodobnosť špecifických dopadov, ktoré nastávajú v priebehu špecifického obdobia alebo počas špecifických podmienok.

Zákon NR SR č. 124/2006 Z.z. o BOZP: Riziko je pravdepodobnosť vzniku poškodenia zdravia zamestnanca pri práci a stupeň možných následkov na zdraví.

Neistota neznamená riziko vo všeobecnosti, ale riziko vzniká pôsobením neistoty na splnení cieľov, ktoré chceme dosiahnuť. Rovnako sa môže jednať o ciele osobné (napr. dostať sa zavčasu na schôdzku), ciele pri vykonávaní projektov (odovzdanie zadaného výsledku projektu včas a s dodržaním rozpočtu) alebo podnikové (zvýšiť čistý zisk podniku, jeho podiel na trhu, vytváranú pridanú hodnotu, optimalizovať podnikové procesy a logistiku, znížiť nekvalitu). [3]

Štandardná ekonomická teória sa zaoberá dosahovaním cieľov trvalo udržateľného rastu a zvýšenia hodnoty podniku pre akcionárov prostredníctvom rastu tržieb (viac predávať) a produktivity (menej míňať). Existuje však ešte jeden dôležitý faktor, ktorý ovplyvňuje výkonnosť podniku: stabilné riadenie rizík. Podniky musia prísť na to, ako riadiť a merať riziko a zamestnávať manažérov rizika, rovnako ako je to pri raste tržieb a produktivity. Pri všetkých rozhodnutiach musia prihliadať na možné hroziace riziká. Rovnako ako u iných činností podniku, je aj na riešenie rizika potrebné vytvorenie plánu na riadenie rizika a rozhodovania v podmienkach neurčitosti. Manažéri sú opatrní a hodnotia riziko v čase krízy, ale len tie najlepšie podniky vedome riadia a hodnotia riziko v časoch prosperity. [4] Je dôležité si uvedomiť, že riziko sa netýka len hlavného predmetu činnosti firmy, ale všetkých oddelení a činností vo firme, preto je potrebný komplexný pohľad na firmu. Riziko sa týka aj strojov, technologických procesov, výpočtovej techniky, budov a ostatnej technickej infraštruktúry podniku, ale taktiež aj údajov, rôznych relevantných dát, know-how, výrobných postupov a pod. Je nevyhnutné vypracovanie plánu riadenia rizika,

1 OGC. 2007. *Management of Risk: Guidance for Practitioners*, In: *The Stationery Office*
2 COOPER – GREY – RAYMOND - WALKER. 2004. *Project Risk Management Guidelines: Manage Risk in Large Projects and Complex Procurements*.s.17.
3 KORECKÝ, M. - TRKOVSKÝ, V. 2011. *Management rizik projektú – se zaměřením na projekty v prúmyslových podnicích*, s. 28
4 KAPLAN, R. S. 2008. *The Centennial Global Business Summit*. [online]

kde sa nastavia rizikové parametre v súlade s podnikovou stratégiou a nepretržite sa vyhodnocujú. Popísanie a poznanie rizík je jediná možná cesta ako úspešne s minimálnymi stratami rizikovú udalosť vyriešiť. Analyzovanie možných situácií a scenárov so záťažovými testami sú dôležité na pochopenie miery rizika a sú východiskom k zvládnutiu alebo vyhnutiu sa rizikovej udalosti. Je to východisko pre krízový manažment podniku.

„Krízový manažment je riadiacou činnosťou ľudí, ktorí plnia manažérske funkcie v špecifickom – krízovom prostredí, odlišujúcom sa od efektívnej prevádzkovej klímy podniku.“ [1]

Konečným stavom je nastolenie rovnovážneho stavu, normálneho fungovania systému, jeho základných prvkov, ktorý sa nazýva stabilita.

1.2.2 Identifikácia rizika

Pripadá nemožné sa pripraviť na krízu, ktorá ešte len nastane a nikto si ani nevie predstaviť aká bude. Napriek tomu existujú jednoduché nástroje, ktoré pomáhajú manažérom naplánovať, ako takúto krízu prekonať a zvládnuť predmetnú kritickú situáciu.

Identifikácia rizika je prvým systematickým krokom v procese manažmentu rizika, ktorého podstatou je odhaliť všetky riziká, ktoré na organizáciu pôsobia z vonkajšieho (strategické riziká) alebo vnútorného prostredia (operatívne riziká). Pri identifikácii rizika je nevyhnutné si uvedomovať axióm, že riziko, ktoré nie je identifikované, nemôže byť ani riadené (ovplyvňované). Čiže môžeme povedať, že ide o kritickú fázu manažmentu rizika, ktorá by mala zahŕňať všetky riziká bez ohľadu na to, či sú, alebo nie sú pod kontrolou organizácie.

Obsahom identifikácie je hľadanie odpovedí na základné otázky:

- aké nepriaznivé udalosti môžu nastať?
- aká je pravdepodobnosť ich výskytu?
- aké budú dôsledky nepriaznivej udalosti?

Cieľom identifikácie rizika v podniku je dať manažérovi podklady pre ovládanie rizika a dať vedeniu spoločnosti relevantné podklady pre riadenie rizika. Súčasťou identifikácie rizika je aj popis jednotlivých rizík, príp. určenie ich príčin a následkov.[2]

Na identifikáciu rizík sa využíva celý rad postupov a techník, vrátane kontrolných zoznamov, posudkov vychádzajúcich zo skúseností a záznamov, vývojových diagramov, výsledkov burzy nápadov (braimstormingu), systémovej analýzy, analýzy scenárov a

1 GOZORA, V. 2000. *Krízový manažment,* s. 182.
2 KORECKÝ, M. - TRKOVSKÝ, V. 2011. *Management rizik projektú - se zaměřením na projekty v prúmyslových podnicích.* s. 89.

systémových inžinierskych techník. Použitá metóda bude závisieť od charakteru uvažovaných činností a od druhu rizika. Pre získanie komplexnejšieho výsledku je vhodné použiť niekoľko navzájom sa dopĺňajúcich metód. [1]

1.2.3 Klasifikácia rizík

Základné kroky procesu hodnotenia rizika

- analýza rizika,
- meranie rizika,
- tvorba rozhodnutí,
- kontrola a monitorovanie. [2]

Analýza rizika - cieľom analýzy je podrobné skúmanie a pochopenie rizík, ich následné hodnotenie určenie ich dopadov na ciele podniku. Východiskom riadenia rizika je oddelenie malých prijateľných rizík od veľkých hrozieb a poskytnutie údajov, ktoré sú relevantné pri hodnotení rizík a zaobchádzaní s nimi. Analýza rizík zahŕňa posúdenie zdrojov rizík, možnosť a druh dopadov na podnik, ich negatívne či možno aj pozitívne dopady, závažnosť týchto dopadov a určenie miery pravdepodobnosti, kedy a za akých okolností tieto udalosti môžu nastať. Často sa analýza rozdeľuje ešte na dve samostatné metódy a to na kvalitatívnu a kvantitatívnu analýzu. Toto delenie sa používa najmä v americkej norme spracovanej PMI (Project Management Institute) a v knihách, ktoré vychádzajú z tejto normy. Prevažuje použitie kvalitatívnej a kvantifikatívnej analýzy ako metódy a nie ich uvádzanie ako fázy analýzy.

Riziko sa analyzuje kombinovaním odhadov následkov a pravdepodobnosti ich vzniku a uvádza sa do súvislosti s existujúcimi kontrolnými opatreniami. Odporúča sa vykonať predbežnú analýzu, aby sa z podrobnejšej štúdie vylúčili podobné riziká alebo riziká s malým dosahom. Ak je to možné, musí sa urobiť zoznam vylúčených rizík, aby sa preukázala úplnosť analýzy rizika. V závislosti od dostupnosti informácií môže byť analýza riešená ako kvalitatívna (slovný opis), semikvalitatívna (expertný popis podložený výpočtami) alebo kvantitatívna (riziko vyjadrené v číselných hodnotách).

Na analýzu rizika sa využívajú podobné metódy, nástroje a techniky ako pri identifikácii rizika. V praxi sa uplatňujú dve základné metódy:

- indukčné metódy „ex ante“ - umožňujú predvídať vznik možnej udalosti a poukazujú na okolnosti, ktoré by mohli vznik udalosti zapríčiniť. Pomáhajú tiež

1 FILIP, S. - ŠIMÁK, L. - KOVÁČ, M. 2011. *Manažment rizika*. s. 89-91.
2 EWRM – Enterprise Wide Risk management - preklad do slovenčiny: VARCHOVÁ – DUBOVICKÁ. 2008. *Nový manažment rizika.* s. 56.

odhadnúť počet a následky udalostí,

- dedukčné metódy analýzy rizika „ex post“ - umožňujú odhadnúť početnosť a následky udalostí na základe udalostí, ktoré sa už v praxi vyskytli a hľadajú súvislosti, ktoré udalosti zapríčinili.

Na analýzu rizika sa v súčasnej dobe používa veľa rôznorodých metód.[1] V praxi sa používajú najmä tieto metódy:

- tradičné metódy:
  - analýza pomocou kontrolných záznamov (Check List Analysis – CLA),
  - rutinné testy (Routine Tests – RT),
  - bezpečnostný audit (Safety Audit – SA),
  - burza nápadov (Braimstorming),
  - metóda čo sa stane ak … (What if Analysis – WFA) – modifikovaný braimstorming,
  - relatívne hodnotenie (Relative Ranking),
  - rýchle hodnotenie (Rapid Ranking – RR),
  - úvodná analýza nebezpečenstva (Preliminary Hazard Analysis),
  - štúdia nebezpečnosti a prevádzkyschopnosti (Hazard and Operability Study – HAZOP),
  - analýza stromom porúch (Fault three Analysis – FTA),
  - analýza nebezpečenstva (Hazard Analysis – HAZAN),
  - analýza stromom nebezpečenstva (Hazard three Analysis – HTA),
  - analýza príčin následkov (Cause Consequence Analysis – CCA),
  - analýza spoľahlivosti človeka (Human Reliability Analysis – HRA),
  - kvantitatívna analýza rizika chemických procesov (Chemical Process Quantitative risk analysis – CPQRA). [2]

Výber konkrétnych metód analýzy rizika závisí od manažérovej dokonalej znalosti problematiky prostredia podniku a to interného aj externého. Náročnosť zvládnutia analýzy determinujú všetky rizikové stavy, dôsledky a následky, ktoré môžu v podniku nastať. Vyhodnocujú sa možné dopady na vlastné objekty a subjekty aj externé. Okrem toho sa pri výbere metód hodnotia existujúce manažérske a technické systémy, postupy riadenia rizika a posudzujú sa ich silné a slabé stránky. [3] Taktiež je dôležité využívanie informácií z

1 KANDRÁČ, J., SKARBA, D. 2000. *Metodický postup na hodnotenie rizík nebezpečných prevádzok a štúdia o podnikoch v SR*. s. 37.
2 NOVÁK, L. a kol. 2010. *Plánovanie zdrojov na riešenie krízových situácií*. s. 278-291.
3 FILIP, S. - ŠIMÁK, L. - KOVÁČ, M. 2011. *Manažment rizika*. s. 93-94.

minulých udalostí.

Analýza rizika nám dáva odpoveď na zásadnú a základnú otázku „V čom môže spočívať skutočný problém?“. Odpoveď nám určí víziu a stratégiu, t.j. stanoví konkrétne ciele s jasne definovaným smerom a časovým horizontom.

Meranie rizika - výstupom z vyhodnocovania rizika je zoznam rizík s prioritami. Ak výsledné riziká patria do kategórie malé riziko alebo prijateľné riziko, možno ich akceptovať s minimálnou ďalšou pozornosťou. Malé riziká a prijateľné riziká treba monitorovať a periodicky preskúmavať s cieľom presvedčiť sa, že stále zostávajú prijateľné. Ak riziká nepatria do kategórie malé riziko alebo prijateľné riziko, treba sa nimi zaoberať a použiť jedno alebo viacero voliteľných opatrení. [1]

Pri meraní rizika pracujeme teda s mierou pravdepodobnosti výskytu jednotlivých rizikových situácií. Pri meraní rizika sa používajú nasledovné prístupy a modely:

- deterministické prístupy (k hodnote jednej premennej sa priradí hodnota inej premennej),
- stochastické prístupy (k hodnote jednej premennej sa priradí hodnota inej premennej, ale vzťahy sú tu náhodné),
- expertné stanovenie rozdelení pravdepodobnosti (subjektívny expertný odhad),
- analytické modely (štandardné teoretické modely),
- situačné modely (ak je problém zložitý – napr. simulácia Monte Carlo).

Výsledkom merania rizika je kvalifikácia a kvantifikácia jednotlivých rizík. Dáva prehľad o tom, aké môžu byť dôsledky rizík, či sú prijateľné, aká je pravdepodobnosť, že k nim dôjde a tiež závažnosť dôsledkov. Určia sa priority riešenia rizika, jednotlivé riziká sa rozdelia na riziká, ktoré je možné akceptovať a na riziká určené na ďalšie riešenie.

Tvorba rozhodnutí - Ide o identifikáciu rozsahu voliteľných opatrení na zaobchádzanie s rizikom, ich posúdenie, prípravu plánov zaobchádzania s rizikom a ich zavedenie. Súčasná prax manažmentu rizika využíva voliteľné opatrenia, ktoré sa pri riadení rizika môžu navzájom kombinovať, nemusia vylučovať, ale taktiež nemusia byť vhodné vo všetkých prípadoch. Medzi najznámejšie opatrenia patria:

- vyvarovanie sa rizika (vyhýbanie sa riziku, prevencia),
- zníženie vierohodnosti výskytu rizika,
- obmedzenie možných následkov udalostí,
- prenos rizika (transfer rizika).

1 Tamtiež. s. 104.

Pri voľbe konkrétnych opatrení sa manažment subjektu musí rozhodnúť, či je potrebné riziko akceptovať, alebo ho odmietnuť na základe hodnotenia rizika, resp. mal by stanoviť či je riziko prijateľné.

Prijateľné riziká by mali byť zahrnuté do politiky manažmentu rizika a malo by sa s nimi v činnosti organizácie počítať. Neprijateľné riziká by mali byť predmetom riadenia alebo subjekty by sa ich mali vyvarovať. [1]

Ako podklad pre riadenie rizika sa vytvoria plány na zaobchádzanie s rizikom. Plány dokumentujú opatrenia, ktoré sa postupne zavádzajú v podniku. V pláne je určená zodpovedná osoba, harmonogram úloh s termínmi, zdroje financovania a prípadné ďalšie ciele.

Rovnako pri príprave rozhodnutia je dôležité vykonať SWOT analýzu podniku identifikáciou:

- Strengths – silné stránky,
- Weaknesses – slabé stránky,
- Opportunities – príležitosti,
- Threats – hrozby a nebezpečenstvá**.** [2]

SWOT analýza podniku ukáže hrozby a nebezpečenstvá a následne aj priority riešenia týchto udalostí.

Kontrola a monitorovanie - Posudzované riziká je nevyhnutné monitorovať a vyhodnocovať. Ak sa mení nebezpečnosť rizík, následne sa mení aj priorita rizík v pláne a časový harmonogram. Vyhodnocujú sa tiež externé a interné faktory, ktoré môžu tiež ovplyvňovať priority riešenia jednotlivých rizík. Plán riadenia rizika sa periodicky musí prehodnocovať a operatívne jednotlivé úlohy meniť a prispôsobovať skutočnosti a reálnej praxi v podniku. Kontrola je neoddeliteľná súčasť plánovania a mala by byť využívaná spoločne s plánovacím procesom. Kontrolnou činnosťou sa porovnáva krízový plán so skutkovým stavom v podniku. Jednotlivé úlohy krízového plánu a ich plnenie sa dokumentujú. Niektoré výsledky a spôsob riešenia rizika sa musia dokumentovať aj na základe právnej úpravy SR špecifickým spôsobom (BOZP, elektro, potravinárstvo, ovzdušie a pod.).

1 FILIP, S. - ŠIMÁK, L. - KOVÁČ, M. 2011. *Manažment rizika*. s. 105.

2 BATE, N. 2009. *Ako poraziť recesiu: Plán na prežitie v podnikaní*. s. 55.

Monitorovanie slúži na získavanie informácií tak, aby boli k dispozícii v reálnom čase. Rovnako v dobrých časoch, ale hlavne na spozorovanie prvých príznakov hroziacej krízy a nerovnováhy. Včasné rozoznanie príznakov začínajúcej krízy umožňuje jej rýchlejšie prekonanie a nastolenie stavu opätovnej rovnováhy. Nerešpektovanie funkcie monitorovania vedie k dodatočným výdavkom, zvýšenému úsiliu a strate času na strategické rozhodnutia. Neskorá, nedostatočná alebo naopak prehnaná reakcia môže vytvoriť ďalšiu krízu alebo situáciu skomplikovať. V každom takomto prípade dochádza k dodatočným stratám spoločnosti.

1.3 Základné požiadavky na manažment rizika

Základné požiadavky na manažment rizika podniku riešia medzinárodne platné normy ISO/IEC 3101:2009 Manažment rizika – hodnotenie rizík, ISO Guide 73:2009, ISO 31000. Možno postupovať aj podľa českej normy Risk management Standard vydanú v r. 2007 v The Institute of Risk Management a normy COSO ERM (Enterprise-wide Risk management 2004). Na Slovensku rieši problematiku rizika podniku slovenská norma STN 010380 Manažérstvo rizika. Táto norma bola spracovaná podľa austrálsko novozélandskej normy AS/NZ 4360:1999. (Normy v podmienkach slovenskej legislatívy nie sú záväzné, ale sú len doporučujúce.) Norma má všeobecné použitie v podniku a je nezávislá od konkrétneho odvetvia. Podľa tejto normy je manažment rizika logická a systémová metóda určovania súvislostí, identifikovania, analýzy, vyhodnotenia, zaobchádzania (riadenia), monitorovania a oznamovania rizík súvisiacich s akoukoľvek činnosťou, funkciou alebo procesom spôsobom, ktorý organizácii umožňuje minimalizovať straty a maximalizovať príležitosti. Posudzovanie rizika rieši taktiež Zákon NR SR č. 124/2006 Z.z. O bezpečnosti a ochrane zdravia pri práci, kde sa rieši ochrana BOZP, čo je vlastne tiež posudzovanie jedného z druhov rizika. V jednotlivých špecifických oblastiach riziko riešia aj ďalšie právne úpravy, napr. Zákon NR SR č. 42/1994 Z.z. O civilnej ochrane obyvateľstva, Zákon NR SR č. 355/2007 Z.z. O ochrane, podpore a rozvoji verejného zdravia, Zákon NR SR č. 152/1995 Z.z. O potravinách, Zákon NR SR č. 261/2002 Z.z. O prevencii závažných priemyselných havárií, Zákon NR SR č. 8/2009 Z.z. o cestnej premávke a ďalšie.

1.3.1 Triedenie a označenie rizík zobrazujeme v nasledujúcej tabuľke.

Tabuľka 1. Triedenie a označenie rizík

ID	*Názov*	*Popis*
B	Bezpečnostné	Krádeže, vandalizmus, sabotáže, poškodenie, strata
F	Finančné	Financovanie, cash flow, dane, dotácie, clá, kurzy, inflácia
G	Garancie a servis	Podmienky záruky a servisu
L	Legislatívne	Regulácie, clá, zákony, know-how, zmluvy
M	Manažérske	Harmonogram, kvalifikácia, management
N	Nákup	Výber dodávateľov, podmienky nákupu subdodávok a materiálu, outsourcing
O	Obchodné	Stratégia, trh, zákazník
T	Technické	Definícia a parametre produktov, vývoj, normy, výroba, skúšky, balenie a preprava

Prameň: vlastné spracovanie

1.4 Bezpečnostné riziká

Bezpečnostné riziko (riziko: možnosť, nebezpečenstvo straty, neúspechu, škody; kombinácia pravdepodobnosti, že nastane neželaná udalosť a následkov neželanej udalosti; kvantitatívne a kvalitatívne vyjadrenie ohrozenia, stupeň alebo miera ohrozenia.) - jav sociálneho charakteru, ktorý má potenciál poškodiť subjekt bezpečnosti, alebo môže mať negatívny dopad na záujmy iného subjektu. [1]

Môže sa vyjadriť *ako* kombinácia:

- pravdepodobnosti (početnosti, vierohodnosti), že dôjde k ohrozeniu chráneného záujmu kriminálnym činom alebo jemu sa blížiacimi dôsledkami činnosti iných ľudí,
- veľkosti možných následkov takejto udalosti.

Pravdepodobnosť, že bude ohrozená integrita určitého subjektu (jedinca, spoločenského útvaru) kriminálnym činom alebo jemu sa blížiacimi dôsledkami činnosti iných ľudí.

Fenomény, ktoré *ohrozujú* bezpečnosť sociálnych subjektov a môžu im spôsobiť ujmu, stratu, škodu, alebo viesť k neúspechu.

Stavy bezpečnostnej situácie (vnútornej i vonkajšej), ktorý prejavy môžu privodiť ohrozenie subjektu bezpečnosti (jedinca, skupiny, štátu, ľudstva).

Z vnútorného hľadiska predstavujú ohrozenie života a majetku občanov, stability politického vývoja a demokratických slobôd v takom rozsahu, že môže dôjsť k zmenám charakteristiky bezpečnosti celého štátu. Riziká majú rôznu mieru pravdepodobnosti

1 Security revue. 2013. [online]

výskytu a rôzny čas, ktorý uplynie od aktivácie až po ohrozenie. [1]

Bezpečnostný manažment *(Security Management)* je špecifická zmysluplná činnosť, zameraná na odvrátenie alebo minimalizáciu bezpečnostných rizík, resp. bezpečnostných ohrození rôznej povahy a príčiny voči životu a majetku občanov, obcí a spoločnosti, obsahujúca v sebe prvky rizikového, krízového, havarijného a hodnotového manažmentu. Obsah bezpečnostného manažmentu je tvorený logickou postupnosťou krokov, vykonávaných na zabránenie vzniku, prejavov alebo minimalizáciu bezpečnostných rizík a ohrození, ktoré vyvolávajú viktimáciu občanov, ohrozujú majetok obcí i spoločnosti, alebo inak pôsobia proti záujmom občanov, sociálnych skupín a spoločnosti. [2] Ide o neustály systémový cyklicky sa opakujúci proces, kde manažment riadi riziká, ktoré ohrozujú podnik. Výsledkom predmetného procesu je zabezpečenie chodu podniku a jednotlivých procesov tak, aby nedochádzalo k turbulenciám a narušeniu stability podniku, nepretržitej prevádzky, produktivity výroby, ochrany životného prostredia, majetku podniku a zamestnancov, dobrého mena podniku a taktiež v neposlednom rade narušeniu života a zdravia. Riadne vyriešená otázka manažmentu rizika podniku spravidla prináša stabilitu, následne zvýšenie produktivity a motivácie zamestnancov. Týmto spôsobom sa zlepšuje meno spoločnosti, znižujú sa ekonomické náklady a zvyšuje sa hodnota podniku, lebo vložené investície sú bezpečnejšie.

1 KULAŠÍK, P. a kol. 2002. *Slovník bezpečnostných vzťahov.* s.42.
2 Security revue. 2013. [online]

2 CHARAKTERISTIKA A ANALÝZA OBJEKTU

Hypermarket je obchodný priestor väčšieho rozsahu, ktorý poskytuje široké spektrum produktov a služieb. V súčasnosti takmer v každej krajine existuje sieť rôznych obchodných domov. Nevyhnutnou súčasťou takéhoto objektu je kompletné zabezpečenie. Zabezpečenie objektu by malo pôsobiť funkčne, ale tiež plniť aj preventívnu funkciu.

2.1 Popis objektu

Analyzovaným objektom je hypermarket HYPER SHOP s.r.o.
Objekt sa nachádza v intraviláne obce, ležiaci v osídlenej zástavbe mesta, celková rozloha objektu 50 x 200 m, t.j. 10000 m^2 celkovej plochy. Pred hypermarketom sa nachádzajú parkovacie plochy pre zákazníkov a za hypermarketom sa nachádza priestor pre zásobovanie tovarom.

Vnútorné priestory hypermarketu možno z hľadiska funkčnosti rozčleniť na:

- administratívne priestory,
- priestory s príslušenstvom pre personál,
- skladové priestory,
- obchodné plochy,
- pridružené priestory určené zákazníkom,
- parkovacie plochy.

2.2 Analýza rizík objektu

Ako prvý krok v analýze rizík je potrebné overiť, či podnik v súčasnosti má vypracované plány alebo štandardné postupy na nakladanie s rizikom vo všeobecnosti alebo na jednotlivé identifikované riziká.

Skúmaný podnik má vypracované základné smernice o BOZP. Dokumentácia obsahuje dokumenty v rámci manažmentu kvality EN ISO 9001:2000. Smernice riadenia rizika podnik nemá vypracované.

V každom prípade je otázka riadenia rizika globálna a je potrebné riadenie rizika riešiť komplexne naprieč celým spektrom rizík v podniku. Keďže sa práca ale venuje bezpečnostným rizikám, budú sa analyzovať a riadiť iba tieto riziká.

Hypermarket a jeho okolie je špecifický priestor, kde sa dajú riziká rozdeliť z

hľadiska dislokácie priestorov na ochranu:

- vonkajších priestorov a bezprostredného okolia hypermarketu,
- vnútorných priestorov hypermarketu,
- perimetrie hypermarketu.

Z časového hľadiska ochrany je možné rozdeliť ochranu na:

- ochranu tovaru v prevádzkovej dobe,
- ochranu tovaru a priestorov mimo prevádzkovej doby.

K predmetnej ochrane okrem ochrany vnútorných priestorov hypermarketu vieme ešte uvažovať aj s ochranou priľahlých priestorov, ako v prevádzkovej dobe, tak aj mimo prevádzkovej doby. Jedná sa o ochranu napr. parkoviska, kde cez deň zabezpečujeme poriadok a ochranu proti rôznym živlom, ktorý sa zaoberajú vykrádaním automobilov, obťažovaním zákazníkov a pod. K tomuto účelu sa spravidla využíva monitorovanie priestorov prostredníctvom systémov PTV.

Podľa závažnosti riziká delíme do nasledovných skupín:

a. prioritné TOP riziká – najväčšia rizikovosť, na prioritné riešenie,
b. akceptovateľné riziká – najnižšia rizikovosť, určené na sledovanie (monitorovanie),
c. ostatné riziká (zostávajúce) – k bližšej analýze alebo ošetreniu následne po „TOP“.

Výstupom z analýzy rizika je register rizík, kde je uvedená kvalifikácia, kvantifikácia a vlastníci rizík, príp. ďaľšie návrhy na ošetrenie a riešenie. Môže byť doplnená o štruktúru rizík, ich upresnenie, výsledky analýz, diagramy a pod.

Dôvodom rozdelenia na hore uvedené tri skupiny je umožniť koncentráciu na najvýznamnejšie riziká v skupine TOP a zároveň znížiť počet rizík pre ďaľšie analýzy a ošetrenie vyčlenením rizík, ktoré sú možné tolerovať. Zoradenie podľa jedného z kritérií sa vykonáva samostatne pre hrozby (kladné hodnoty, vzostupne) a príležitosti (záporné hodnoty, zostupne).[1]

1 KORECKÝ, M. - TRKOVSKÝ, V. Management rizik projektú – se zaměřením na projekty v prúmyslových podnicích, s. 344

Tabuľka 2. Prioritné TOP riziká

ID	*Riziko*	*Popis*	*Návrh vlastníkov*	*Kvantifikácia (%)*
1	Únik informácií	Únik informácií o dodávateľoch, odberateľoch, zákaziek, tovare	Manažment	25
2	Únik know-how	Vzťahy, logistika, personalistika	Manažment	20
3	Ohrozenie života, zdravia	Elektro, plyn, požiar, bezpečnosť pri práci atď.	BOZP	18
4	Krádež tech.infraštruktúry	Server, klientske stanice, router	Správca IT	15
5	Poškodenie infraštruktúry	Server, klientske stanice, router	Správca IT	10
6	Krádež hotovosti	Tržby, pokladnica	EO	5
7	Poškodenie tovaru		Skladníci, predavači	4
8	Krádež tovaru		Skladníci, predavači	3
9	Poškodenie vybavenia		Skladníci, predavači	3

Prameň: vlastné spracovanie

Tabuľka 3. Akceptovateľné riziká

ID	*Riziko*	*Popis*	*Návrh vlastníkov*	*Kvantifikácia (%)*
1	Záplavy		Skladník	20
2	Poškodenie budovy		Skladník	30
3	Poškodenie vybavenia		Skladník	50

Prameň: vlastné spracovanie

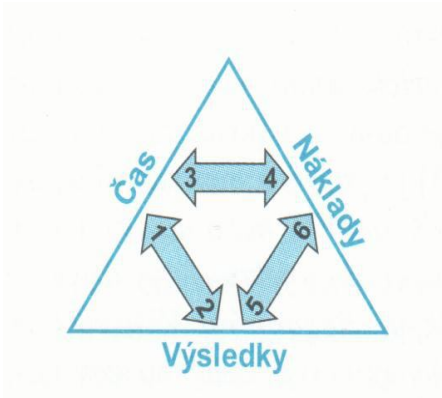
Tabuľka 4. Ostatné riziká

ID	*Riziko*	*Popis*	*Návrh vlastníkov*	*Kvantifikácia (%)*
1	BOZP		BOZP	5
2	Spôsobilosť technickej infraštruktúry		Management	20
3	Spôsobilosť vybavenia budovy		Management	15

Prameň: vlastné spracovanie

2.3 Riadenie rizika objektu

Register prioritných TOP rizík nie je nemenný. Dokument sa vyhotovuje primárne v elektronickej podobe, lebo sa jedná o dynamický dokument. Ako sa vyvíja proces manažmentu rizika, tak sa postupne mení aj register rizík. K registru rizík sa v procese riadenia rizika priraďujú informácie relevantné pre riadenie rizika ako a kedy môže udalosť nastať, jej frekvencia (ak sa dá predpokladať), spúšťač rizikovej udalosti – trigger, stav rizika. Následne sa rieši spôsob ošetrenia rizika. Stanovuje sa možná – preferovaná a záložná stratégia na riziko, a taktiež konkrétna akcia pre implementáciu stratégie (plánovaná a/alebo už vykonané). Na vypracovanie a riešenie každého konkrétneho rizika je potrebný čas a náklady. Je potrebné posúdiť, či vynaložený čas, priame a dodatočné náklady sú primerané dosiahnutým výsledkom.



zdroj: KORECKÝ, M. - TRKOVSKÝ, V. Management rizik projektů – se zaměřením na projekty v prúmyslových podnicích, s. 324

Obrázok 1. Vzájomné pôsobenie základných dimenzií rizika

Analýza nákladov a prínosov (cost/benefit analysis - CBA) porovnáva celkové očakávané náklady oproti celkovým očakávaným prínosom pre skúmané varianty. Vzájomné pôsobenie jednotlivých základných zložiek a dimenzií rizika je zobrazené na obrázku č. 1. Na základe zhodnotenia vzájomného pôsobenia rizík vykonávame analýzu nákladov a prínosov a teda sa na základe tejto metódy môžeme napríklad rozhodnúť:

- či má zmysel do rizika vstupovať (pokiaľ je možná voľba),
- či má vôbec zmysel riziko ošetrovať (náklady na ošetrenie rizika by nemali byť väčšie ako dosiahnuté prínosy),
- aká z foriem alebo ktorý z postupov ošetrenia rizika je najvýhodnejší.

Nezávislá objektívna analýza má zahrnúť náklady a prínosy pre všetkých zainteresovaných (shareholders), teda všetkých, na ktorých môžu mať hodnotené varianty

pozitívny alebo negatívny vplyv. Tento postup je vyžadovaný najmä v prípadoch, keď majú hodnotené varianty vplyv na bezpečnosť alebo na životné prostredie.[1] V prostredí hypermarketu sa berú do úvahy náklady, ktoré majú vplyv na ziskovosť s cieľom dosiahnutia najväčšieho zisku. Analýza sa vykonáva kvantitatívne vyjadrením v peňažných jednotkách, kde sa porovnávajú výnosy a náklady vyjadrené ako peňažné toky v čase, ktoré sa diskontujú a počíta sa čistá súčasná hodnota (NPV – Net Present Value) a vnútorné výnosové percento (IRR – Internal Rate of Return).[2] Vypočítané hodnoty je potrebné porovnať s nulovou variantou, kedy sa žiadne opatrenie nevykonáva.

2.4 Technická ochrana objektu a priľahlého pozemku

Objekty chránime kombináciou a spolupôsobením rôznych foriem ochrany. Základné formy ochrany objektov sú klasická ochrana, režimové opatrenia a technická ochrana objektu. Technická ochrana doplňuje a podporuje klasickú ochranu objektu. Kombináciou a integráciou rôznych druhov a foriem ochrany objektu sa zvyšuje efektívnosť ochrany objektu. Systémy technickej ochrany objektov a majetku sú vytvorené súborom detekčných, vyhodnocovacích, zobrazovacích, signalizačných a prenosových zariadení, ktoré ako jeden ucelený systém detekujú a signalizujú poplachový alebo iný neštandardný stav. Signalizácia neštandardného a poplachového stavu je signalizovaná lokálne priamo v objekte a následne je poplachový stav prenášaný na stredisko registrácie poplachov za účelom zabezpečenia zásahu na chránenom objekte.

Druhy systémov technickej ochrany:

EPS – elektrická požiarna signalizácia – elektrický systém, ktorý je určený na včasnú detekciu a signalizáciu poplachového stavu pri požiari v objekte spravidla v mieste obsluhy

PSN – poplachové systémy na hlásenie narušenia – elektrický systém, ktorý je určený na detekciu a signalizáciu poplachového stavu pri vniknutí do stráženého priestoru a/alebo objektu, narušenie predmetu pri predmetovej ochrane a taktiež v neposlednom rade na signalizáciu poplachového stavu pri núdzovom stave, napr. pri prepadnutí objektu

PTV – priemyselná televízia – slúži na zaznamenanie skutku a správania páchateľa v objekte

1 KORECKÝ, M. - TRKOVSKÝ, V. 2011. *Management rizik projektú – se zaměřením na projekty v prúmyslových podnicích.* s. 324
2 FOTR, J. - SOUČEK, I. 2005. *Podnikatelský záměr a investiční rozhodování.* s 57.

SKV – systémy kontroly vstupu – elektronická kontrola oprávnenia vstupu osôb a evidencia prítomnosti, napr. z dôvodu možnosti evakuácie objektu

Integráciou týchto rôznych systémov do jedného celku získame efektívny systém ochrany objektu. Základom však je vytvorenie kvalitnej klasickej ochrany a systému režimových opatrení. Technická ochrana dopĺňa klasickú a režimovú ochranu - nenahrádza ju. Spolupôsobením týchto jednotlivých prvkov vzniká jednotný systém, ktorý sa nazýva bezpečnostný systém podniku. Bezpečnostný systém podniku je spravidla tvorený účelným usporiadaním a používaním mechanických a technických prostriedkov, organizačných a režimových opatrení a disponibilných ľudských zdrojov.[1]

1 LOVEČEK, T. - NAGY, P. 2008. *Bezpečnostné systémy: Kamerové bezpečnostné systémy*. s. 253

II. PRAKTICKÁ ČASŤ

3 NÁVRH TECHNICKEJ OCHRANY OBJEKTU A POZEMKOV

Na základe vykonanej analýzy, zo skúmaných dát, z výsledkov a zistených skutočností vyvodzujeme závery s návrhom možného riešenia riadenia rizika a doporučením k aplikovaniu v praxi za účelom zvýšenia bezpečnosti objektu a zníženia rizík, nebezpečenstiev a možných stavov neurčitosti. Používame metódy a techniky na získanie relevantných dát slúžiacich k analýze, ktoré boli východiskom k riešeniu danej problematiky a impulzom pre vykonávanie zberu a skúmaniu dát.

3.1 Návrh systému riadenia rizika

Na začiatku návrhu systému riadenia rizika v objekte je potrebné vykonanie bezpečnostného posúdenia objektu hypermarketu a jeho okolia. Bezpečnostným posúdením objektu sa zisťuje riešenie bezpečnosti a opatrení na zabezpečenie funkčnosti a účinnosti bezpečnostných opatrení a miera bezpečnosti alebo nebezpečnosti v prípade vzniku jednotlivých hrozieb ako narušenia rovnovážneho stavu. Ide posúdenie súboru postupov a opatrení, ktoré sú uplatňované v činnosti podniku. V rámci bezpečnostného posúdenia sú posudzované technické, technologické, informačné, personálne opatrenia, spôsob nakladania s rizikom a postupy pri ich vzniku, dokumentovanie rizík, rozpracovanosť systému riadenia rizika a funkčnosti manažmentu. Do bezpečnostného posúdenia podniku sú zahrnuté interné audity bezpečnosti a taktiež externé služby poskytované dodávateľským spôsobom. Bezpečnostné posúdenie podniku je objektívne posúdenie skutkového stavu riadenia rizika v podniku formou komplexnej analýzy bezpečnosti podniku s návrhom na odstránenie nedostatkov a ich riešenia. Bezpečnostné posúdenie podniku je vykonávané v zmysle STN, ISO a EN noriem. Posudzuje sa súlad a dodržiavanie predmetného súboru noriem, zhodu s legislatívou, rozpracovanosť a dodržiavanie internej metodiky. Ide nie len o stanovenie dodržiavania minimálneho rozsahu povinností stanovených legislatívou a právnymi predpismi, ale po detailnej analýze sa odhaľujú aj tie nebezpečenstvá a ohrozenia, ktoré nie sú priamo riešené právnymi predpismi a legislatívou. Zamestnávatelia a manažment spoločností si v mnohých prípadoch neuvedomujú, že všeobecne záväzné právne predpisy stanovujú len minimálny rozsah povinností, stanovujú návod ako sa vyhýbať jednotlivým nebezpečenstvám a ohrozeniam a predsa len svojim rozsahom nemôžu pokrývať všetky špecifiká jednotlivých procesov v spoločnostiach akokoľvek podrobne sú tieto predpisy rozpracované. Práve z tohto dôvodu je potrebná čo najdetailnejšia analýza konkrétnych reálií a špecifík skúmaného objektu, aby sa odhalili tie nebezpečenstvá a ohrozenia, ktoré nie sú riešené v bezpečnostných predpisoch a bolo ich

možné riešiť a odstraňovať samostatne.

3.2 Návrh riešenia klasickej ochrany

Analýzou jednotlivých prvkov klasickej ochrany bolo zistené, že sú navrhnuté a použité štandardným spôsobom. Mechanické ochranné prostriedky sú použité s cieľom sťaženia alebo zabránenia prístupu do podniku a jeho priestorov, kde zabraňujú vstupu a manipulácii s infraštruktúrou podniku, výrobnými prostriedkami a tovarom. Prvky klasickej ochrany mechanickou odolnosťou a pevnosťou použitých materiálov chránia predmety ochrany, na ktoré sú určené. Zahŕňajú oplotenie objektu, jeho dôležitých častí, zamrežovanie okien a ochranné fólie na ich sklenených výplniach, mechanicky a protipožiarne odolných dverí, zámky a uzamykacie mechanizmy, trezor a príručné pokladne. Zahrňujú vonkajšiu perimetrickú plášťovú ochranu objektu, plášťovú ochranu budovy podniku a predmetovú ochranu jednotlivých predmetov záujmu a záujmových miest. Nie sú však zahrnuté do komplexného systému ochrany objektu a z tohto dôvodu samotné eliminujú riziko len v minimálnej miere. Z tohoto dôvodu je potrebné ich zakomponovanie a zahrnutie do celkového Bezpečnostného projektu riešenia rizika v objekte.

3.3 Návrh riešenia režimovej a fyzickej ochrany objektu

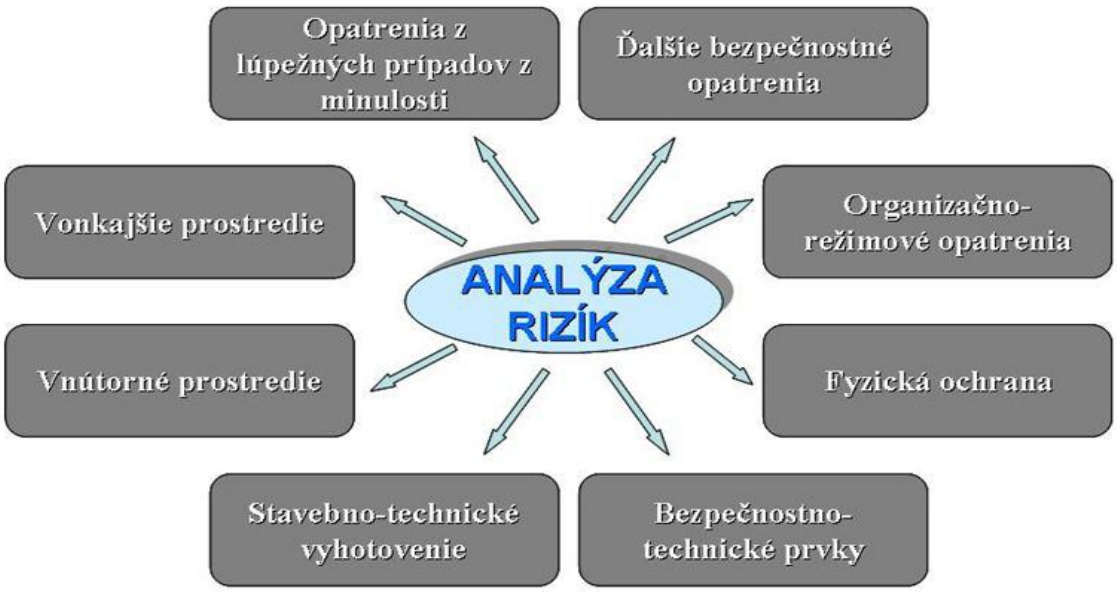
Režimová ochrana objektu je súhrnným označením pre vytvorené smernice a nariadenia, ktoré upravujú pravidlá a oprávnenia vstupu a pohybu osôb v jednotlivých častiach objektu. V predmetnej ochrane hypermarketu sa týkajú súhrnu obmedzení vstupu osôb a ich riadenia technickými prostriedkami, personálnymi opatreniami a kontrolou dodržiavania opatrení zo strany fyzickej ochrany objektu. Súhrn opatrení je tvorený kontrolou pohybu osôb (vstupný a výstupný režim), materiálový a tovarový režim (príjem, evidencia tovaru a materiálu), organizačné opatrenia (prevádzkový režim) a kľúčový režim (klúče, karty, biometria a prideľovanie oprávnení). Oprávnenia a obmedzenia majú časovú a priestorovú dimenziu. Prioritou súhrnu vytvorených opatrení je minimalizácia ľudského faktoru, preto navrhujeme všetky režimové opatrenia v objekte riešiť autonómne jednotlivými prvkami technických systémov a fyzickú ochranu eliminovať len na minimálne možnú mieru. Navrhované riešenie síce znamená väčšie počiatočné náklady na zavedenie technických opatrení oproti kompletnej fyzickej ochrane, ale eleminuje ľudský faktor a nepochybne v značnej miere znižuje prevádzkové náklady spojené s fyzickou ochranou objektu. Úplné zrušenie fyzickej ochrany pri požiadavke na kvalitnú ochranu

objektu však nie je možné, pretože iba fyzická ochrana ako jediný prvok systémov ochrany je schopná vykonať zásah a odstániť tým hroziace riziká, zmariť zámery a plány narušiteľa a vykonať bezprostredné opatrenia smerujúce k nastoleniu rovnovážneho stavu bezpečnosti v objekte. Cieľom je zabrániť útokom na osoby a majetok alebo aspoň tento útok odstrániť a potlačiť jeho následky s prihliadnutím na špecifiká predmetného objektu.

3.4 Návrh riešenia technickej ochrany

Technická ochrana objektu zahrňuje súhrn technických opatrení, ktoré sa skladajú z jednotlivých subsystémov a sú zakomponované do komplexného systému technického riešenia zabezpečenia objektu. Zahrňuje systém PSN, PTV a SKV s nadväznosťou na iné systémy, ako napr. automatizáciu budov, telefónnu ústredňu, ovládanie prívodov elektriky a vody. Prvky technickej ochrany objektu sú najspoľahlivejšie a najťažšie prekonateľné. Vytvárajú efektívny a najúčinnejší prvok riadenia rizika objektu.

Analýza rizík



Zdroj: Security revue, [online] http://www.securityrevue.com, *22.4. 2013*

Obrázok 2. Analýza rizík

Návrhu technického riešenia zabezpečenia objektu a eliminácie rizík predchádza uvedomenie si, zisťovanie a analyzovanie jednotlivých rizík. Vplyv a druhy jednotlivých druhov rizík pôsobiacich na podnik sú uvedené na obrázku č. 2. Analyzovali sme jednotlivé riziká pôsobiace v internom a externom prostredí podniku, stavebno technické vyhotovenie infraštruktúry podniku, bezpečnostno technické opatrenia a prvky, režimové opatrenia a prvky fyzickej ostahy objektu. Analýzou boli zistené riziká vyskytujúce sa v minulosti, hroziace možné riziká v súčasnosti a budúcnosti. Na základe analýzy boli tieto jednotlivé riziká riešené technickou a režimovou ochranou objektu za účelom minimalizovania rizika a nebezpečenstiev. Zanedbateľné riziká vzhľadom k ich rozsahu neeliminujeme, ale je potrebné v budúcnosti pravidelne prehodnocovať popísané riziká z dôvodu, že v súčasnosti zanedbateľné riziko sa môže v budúcnosti stať podstatným rizikom ohrozujúcim podnik alebo jeho zamestnancov. Z tohoto dôvodu vedieme index rizík prioritne v elektronickej podobe, aby sa dal jednoducho v prípade potreby meniť.
TOP riziká sú riešené v systéme komplexnej ochrany pred rizikami.

4 Hardvérové riešenie technológií

Cieľom tejto kapitoly je vytvorenie návrhu hardverového riešenia zabezpečenia hypermarketu s integráciou rôznych podsystémov do jedného celku. Účinnú a efektívnu ochranu objektu zabezpečíme vhodným usporiadaním a vzájomnou kombináciou jednotlivých podsystémov, ktoré vzájomne potom tvoria jeden ucelený systém s definovanými a danými logickými vzájomnými vťahmi medzi nimi. Podsystémy zabezpečenia budovy tvoria systémy EPS, PSN, PTV a SKV. Týmito systémami vytvoríme komplexnú štruktúru zabezpečenia objektu hypermarketu vrátane perimetrie objektu.

Návrh predpokladá použitie niekoľkých samostatne funkčných a na sebe nezávislých systémov, čím sa zabezpečí vysoká miera spoľahlivosti a prevádzkyschopnosti. Nie je prípustná situácia, že prípadná porucha alebo nedostatočné riešenie niektorého z prvkov by mohlo spôsobiť ohrozenie bezpečnosti a komplexnej ochrany celého objektu alebo niektorej samostatnej sekcie objektu. Optimálne navrhnuté jednotlivé podsystémy a ich integrácia zefektívňuje ochranu objektu, zvyšuje úroveň kontroly, čím sa dosahuje vysoká miera prehľadnosti jednotlivých častí systému a identifikovateľnosti konkrétnych udalostí s vytvorením centrálnych väzieb podsystémov v nadradenom systéme.

4.1 Poplachový systém na hlásenie narušenia

Majetok spoločnosti, zdravie a život zamestnancov chráni systém PSN. Systém PSN slúži na včasnú detekciu neštandardného stavu v objekte pri vlámaní alebo prepadnutí objektu a následného signalizovania poplachového stavu na stredisko registrovania poplachov za účelom vykonania zásahu na chránený objekt. Poplachový signál po narušení objektu je signalizovaný v stredisku registrácie poplachov, ktoré vyšle na narušený objekt zásahovú jednotku. Účelom PSN (okrem preventívnej funkcie) nie je zabrániť neštandardnému stavu, ale vyslaním zásahovej jednotky najmä účinne a operatívne zabrániť vzniku väčších škôd a ich možný vplyv na funkčnosť a prevádzku podniku – v prípade narušenia mimo pracovnej doby podniku a vykonať opatrenia pre maximálnu ochranu životov a zdravia pracovníkov – v prípade signalizovania prepadnutia v prevádzkovom čase podniku.

Hypermarket navrhujeme zabezpečiť systémom PSN. Pre daný objekt navrhujeme riadiace zariadenie GALAXY Dimension 520, indikačné zariadenie MK-8, výrobca Honeywell (obrázok č. 3). Ide o moderné, plne programovateľné RZ PSN novej generácie,

ale dlhoročne osvedčenej rady výrobkov. V základnej zostave má 16/32 – slučiek a je možnosť ich rozširovania pridaním max. 63 expanderov na 520/1040. Jednotlivé slučky môžu byť pridelené do 32 programovateľných oblastí, ktoré môžu byť použité ako vmútorné, vonkajšie, požiarne, oneskorené, okamžité, sledované, 24 hodinové, dvojité /49 funkcií vstupov/. Každej zóne, užívateľovi a správe o stave RIZ je priradený osobitný popisovač a priraďované ľubovoľné texty. Systémové parametre sa editujú v PSN prostredníctvom programovacieho nástroja od výrobcu zariadenia.

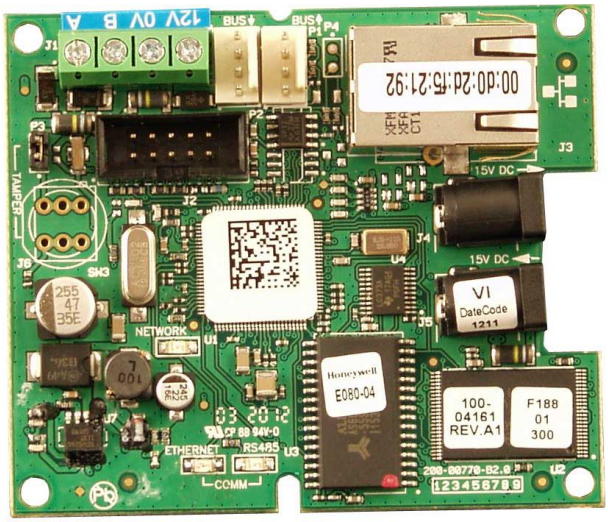
Zdroj: HONEYWELL, [online] http://www.security.honeywell.com

Obrázok 3 .Systém Galaxy GD-520

Každá oblasť v systéme môže byť priradená ktorejkoľvek časti a každá časť môže byť osobitne zapínaná, vypínaná a zobrazovaná na klávesniciach s následným rozdelením konkrétnej lokalizácie poplachového stavu na výstupnom zariadení. V predmetnom použití je ponechaná dostatočná systémová rezerva na ďaľšie prípadné rozširovanie a modifikáciu systému. RIZ je ovládaná max. 999. rôznymi kódmi s voliteľnými oprávneniami obsluhy, ktoré môžu byť 4 až 6 ciferné. Záznamník udalostí zaznamenáva všetky systémové udalosti /1500 poplachových udalostí, 1000 udalostí kontroly vstupu/, ktoré je možné si prezerať na indikačnom zariadení PSN /iba oprávnené osoby, resp. technik pomocou PC/. Taktiež sú zaznamenávané stavy o potiažach systému v samostatnom záznamníku /napr. výpadok 230 V, slabý akumulátor, poškodenie rozvodov PSN atď./ V prípade potreby môže byť použitá dotyková klávesnica, 32 klasických LCD klávesníc typu MK-7 alebo MK-8. RZ je homologované Políciou do objektov vyššieho rizika. LCD klávesnica umožňuje komfortnú

obsluhu systému s využitím všetkých vlastností systému, ako napr. prezeranie záznamov v histórii, zmena, vymazávanie a editovanie kódov, zobrazovanie potiaží systému, prehľadné zobrazovanie celkového a podrobného stavu poplachového systému na hlásenie narušenia. Umožňuje svojimi vlastnosťami prehľadnú a pritom jednoduchú obsluhu.

Integračný prvok je interný modul RS-232, externý modul E054 na krátke vzdialenosti alebo do siete LAN prostredníctvom ethernet modulu E080 (obrázok č. 4). Naprogramovanie systému sa zabezpečuje prostredníctvom programu technika Galaxy Servicing Suite prostredníctvom rozhrania RS-232, LAN alebo príp. cez USB cez prevodník USB/RS-232. U rady Flex je možné pripojenie aj priamo na USB zbernicu.



Zdroj: HONEYWELL, [online] http://www.security.honeywell.com

Obrázok 4. Ethernet modul Galaxy E080

Na zabezpečenie objektu v nočnej dobe (mimo prevádzkových hodín) sa bežne používajú detektory technológie PIR. Keďže je našou úlohou zameranie na kvalitu zabezpečenia, tak použijeme duálne detektory, kde detekujú pohyb v priestore dva nezávislé detektory jeden PIR a druhý MW. Na zvýšenie bezpečnosti doplnené funkciou anti-masking.

S ohľadom k daným požiadavkám použitie s montážou na stenu navrhujeme duálne detektory s funkciou anti-masking typu Tower-12, výrobca Visonic (obrázok č. 5).

Zdroj: VISONIC Ltd., [online] http://www.visonic.com

Obrázok 5. Detektor PIR+MW AM TOWER-12

S montážou na strop navrhujeme použitite detektorov RK-150DT-G3, výrobca Risco (obrázok č. 6). Detektory PIR rozdeľujú priestor vertikálne aj horizontálne a vytvoria detekčné zóny, kde lokalizujú poplachový stav. Nezávisle od PIR senzora je v detektore nezávislý MW detektor a tiež snímač anti-maskingu. Pri vyhodnotení poplachového stavu detektory sa zopnú a tým vyvolajú v RZ poplachový stav v príslušnej zóne náležiacej do danej oblasti.

Zdroj: RISCO LTD., [online] http://www.riscogroup.com

Obrázok 6. Detektor PIR RK-150DT

Na zabezpečenie plášťovej ochrany objektu na okná do výšky 3 m od terénu sa v praxi používajú magnetické senzory a/alebo detektory deštrukcie skla. Magnetické senzory sú základným elementom plášťovej ochrany objektu. Ich funkciou je detekcia otvorenia otvorenia okien a dverí, resp. aj inštalačných skriniek apod. Okrem okien sa umiestňujú na všetky vstupy do objektu – dvere a brány a taktiež na vstupy do jednotlivých sekcií objektu,

ktoré budú samostatne ovládané a zapínané pod ochranu.

Magnetické senzory pracujú na princípe priblíženia permanentného magnetu umiestneného na pohyblivej strane okna k jazýčkovému relé zatavenému v sklenenej vákuovej banke umiestnej na pevnej časti okna, kde sa vplyvom pôsobenia magnetizmu zopnú kontakty a takýmto spôsobom je signalizovaný štandardný stav a po následnom oddialení permanentného magnetu od jazýčkového relé je vyvolaný poplachový stav. Jazýčkové relé môžu byť vo vyhotovení NC, NO alebo s prepínacím kontaktom NO/NC. V predmetnej aplikácie navrhujeme použitie senzorov z produkcie Honeywell, a to povrchových magnetických senzorov typu MPS-20 a MPS-45 a závrtných magnetických senzorov typu MPS-9. Všetky navrhované senzory sú vo vyhotovení s kontaktom typu NC (obrázok č. 7).

Zdroj: HONEYWELL, [online] http://www.security.honeywell.com

Obrázok 7. Magnetické detektory MPS-20, MPS-45, MPS-9

Na zabezpečenie brán objektu navrhujeme masívne odolné magnetické senzory z produkcie SATEL typy B-4M, B-4L a B-4S, ktoré sú umiestnené v hermeticky uzatvorenom kovovom kryte a sú určené na povrchovú montáž. Vývody zo senzorov sú pevne osadené a sú vedené v kovovej chráničke (obrázok č. 8).

Zdroj: SATEL Sp. z o.o., [online] http://www.satel.pl

Obrázok 8. Magnetické detektory M-4S, M a L

Okná a presklené časti plášťa budovy navrhujeme zabezpečiť detektormi deštrukcie skla, ktoré detekujú prostredníctvom duálneho audiodetektora špecifickú frekvenciu a audio sekvenciu rozbitia skla a sú vhodné aj na sklá s tabulovým a tvrdeným sklom do hrúbky 10 mm, vstvovo lepeným sklom do hrúbky 14 mm, drátové sklo do hrúbky 6 mm, vákuové sklá a sklá s bezpečnostnými fóliami do hrúbky 6 mm s hrúbkou fólie max. 0,3 mm, dosah detektora 7,6 m typ FG-1625TAS. Detektory majú krytie do vnútorného prostredia. (obrázok č. 9).

Zdroj: HONEYWELL, [online] http://www.security.honeywell.com

Obrázok 9. Detektor deštrukcie skla FG-1525TAS

\ .DPRO

PRO-100 uchytené na konzole ADPRO PRO-CMB-W, výrobca Xtralis (obrázok č. 10). Detekčná charakteristika je 120x2,9 m a preto takáto záclonová charakteristika je ideálna na pokrytie veľkých vonkajších plôch. Vhodné sú na aplikácie komerčného charakteru, ale rovnako aj na Hi-Security aplikácie. Montážna výška je 2,4 – 4 m za účelom umiestnenia

detektorov mimo dosah a zabráneniu ich poškodenia. Detektor má unikátnu anti-vandal technológiu, ktorou vyhodnocuje zmenu zamierenia detektora a detekčnej plochy. Pri inštalácií sa na zameranie detekčnej plochy využije zameriavací hľadáčik ADPRO AD-851, ktorým nastavíme požadované zamierenie detektoru za účelom kvalitného pokrytia priestoru exteriéru.

Zdroj: XTRALIS Pty Ltd., [online] http://www.xtralis.com

Obrázok 10. Vonkajší detektor PIR ADPRO PRO-100

Na zabezpečenie objektu v dennej dobe navrhujeme do miestnosti obsluhy (miestnosť SBS) umiestniť tiesňové tlačítko a na pokladničné miesta tiesňové tlačítka a detektory poslednej bankovky. Navrhujeme použitie osvedčeného výklopného núdzového hlásiča SENTROL 3040 z produkcie Honeywell (obrázok č. 11). Hlásič sa umiestňuje na miesta, kde sa manipuluje s hotovosťou, v miestnosti obsluhy s takou polohou, ktorá vyhovuje obsluhe. Typické umiestnenie je zo spodnej strany pracovnej dosky stola (napr. pod pokladňou alebo pod pohyblivým pásom s tovarom), aby hlásič nebol viditeľný. Pripevňuje sa alternatívne vo zvislej alebo vodorovnej polohe. Po uvedení hlásiča do poplachového stavu zostane svietiť červená LED dióda pamäti poplachu za účelom neskoršej identifikácie zdroja poplachu, napr. v prípade falošného poplachu spôsobeného obsluhou. Reset pamäte sa vykonáva diaľkovo z riadiaceho zariadenia PSN.

Zdroj: HONEYWELL, [online] http://www.security.honeywell.com

Obrázok 11. Detektor SENTROL 3040

Na zvýšenie bezpečnosti obsluhy navrhujeme umiestnenie aj tiesňového hlásiča snímača poslednej bankovky, ktorý pracuje na princípe, že posledná bankovka musí vždy zostať v priečinku hotovostnej zásuvky. Ak sa táto posledná bankovka vyberie, spoja sa kontakty snímača a je zasielaný poplachový stav prepadnutia. Navrhujeme použitie snímača typ DC-301 (obrázok č. 12). Je určený k montáži do vnútorného prostredia a má kompaktný kryt pre jednoduchú montáž.

Zdroj: HONEYWELL, [online] http://www.security.honeywell.com

Obrázok 12. Detektor DC-301

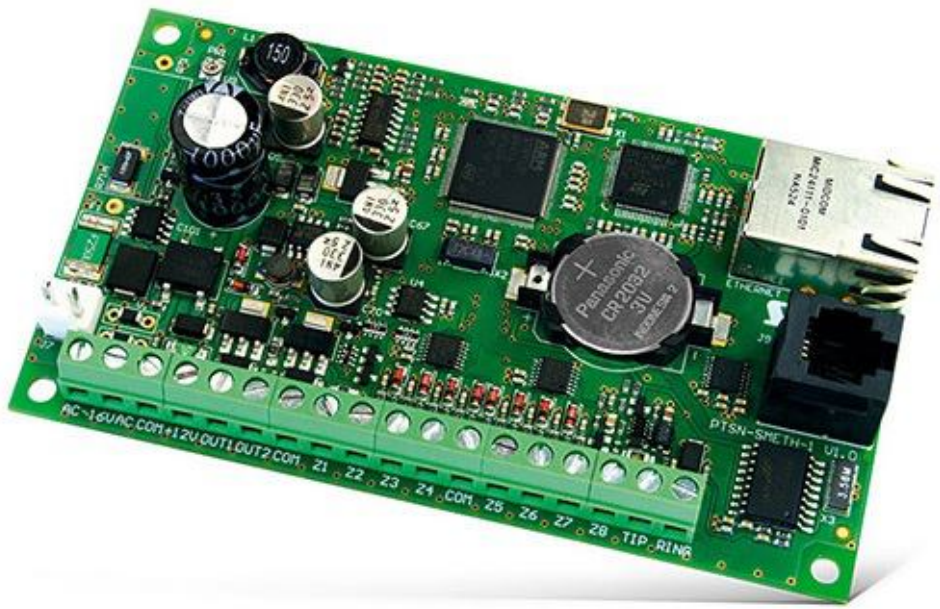
Lokálna signalizácia je vonkajšou zálohovou sirénou SA-11, výrobca Cerber (obrázok č. 13). Vonkajšia siréna je robustná, oplechovaná a zvonku plastová, odolná proti jej znefunkčneniu zapenením. Dvojité opláštenie zabezpečuje väčšiu mechanickú odolnosť a pri pokuse o jej narušenie obsahuje sabotážny tamper kontakt, ktorý už pri pokuse o jej poškodenie signalizuje takýto stav do RZ, ktoré ho samostatne vyhodnocuje ako sabotáž zariadenia. Mechanizmus tampera je vyhotovený spôsobom, že vyhlási poplach pri otvorení sirény a taktiež aj pri jej odtrhnutí (napr. vypáčením) od steny. Rovnakým princípom činnosti sú štandardne chránené všetky navrhnuté komponenty PSN, ktoré signalizujú stav sabotáže aj keď je zariadenie vypnuté. Spôsob vyhodnocovania sabotáže je taký, že sabotáž je vyhlásená aj pri skrate alebo prerušení kabeláže PSN.

Zdroj: ROEL electronics S.A., [online] http://www.roel.ro

Obrázok 13. Siréna

Poplachový stav s ohľadom na zabezpečenie zásahu sa navrhuje prenášať na stredisko registrácie poplachov (SRP), kde je zabezpečený nepretržitý dohľad nad stráženým objektom a v prípade poplachového stavu vysielaná zásahová jednotka za účelom vykonania zásahu na chránenom objekte. Na pripojenie na SRP s ohľadom na bezpečnosť prenášaných dát navrhujeme modul ETHM-2, výrobca Satel (obrázok č. 14). Tento modul transformuje dáta vo formáte Contact-ID do internetu, prostredníctvom ktorého budú prenášané signály na SRP formou simulácie telefónnej linky pre riadiace zariadenie PSN. Okrem vo všeobecnosti najpožívanejšieho formátu telefónnej komunikácie Contact-ID ethernet modul umožňuje niekoľko ďalších formátov telefónnej komunikácie ako sú Ademco slow aj express, Silent Knight fast, Radionics 1400 s paritou

aj bez parity a formát SIA. Po prevode telefónneho formátu zašifruje dáta a následne ich zasiela cez sieť TCP/IP na SRP. Každú udalosť SRP potvrdí. Okrem už popísaného prevodníka modul taktiež obsahuje 8 klasických NO/NC vstupov a 4 výstupy za účelom pripojenia ostatných zariadení alebo nepoplachových aplikácií v objektoch. V predmetnom použití sú to sabotážne výstupy z jednotlivých samostatných systémov a tiež všetky poplachové stavy, nakoľko telefónnu komunikáciu navrhujeme použiť na zabezpečenie duálnej prenosovej cesty na SRP. Modul má zabudovaný samostatný pulzný zdroj s možnosťou pripojenia záložného akumulátora. S ohľadom na bezpečnosť a kvalitu navrhujeme zálohovanie záložným aku AGM 12V 7 Ah, ktorý priamo doporučuje aj výrobca.



Zdroj: SATEL Sp. z o.o., [online] http://www.satel.pl

Obrázok 14. Komunikačný modul ETHM-2

Ako duálny prenos poplachových stavov na SRP navrhujeme použitie interného telefónneho komunikátora zabudovaného v RZ Galaxy Dimension. Navrhovaný formát prenosu na SRP Contact-ID, príp. SIA. Komunikáciu s ostatnými zariadeniami a systémami v budove zabezpečí rozširovací modul Galaxy Rio, výrobca Honeywell prostredníctvom zbernice RS-485. Celý systém je zálohovaný proti výpadkom elektrického prúdu záložnými akumulátormi technológie AGM, samostatne pre riadiace zariadenie PSN a samostatne pre vonkajšiu zálohovanú sirénu. Systém je monitorovaný a údaje z neho zaznamenávané v

troch na sebe nezávislých zariadeniach, a to v riadiacom zariadení PSN, integračnom systéme a taktiež v stredisku registrácie poplachov.

Inštalácia kabeláže je realizovaná vodičmi SYKFY 3x2x0,5 (alternatívne použitie tieneného vodiča FTP cat 5+), hlavné káblové rozvody zbernicou RS-485 vodičom JYSTY 2x2x0,8 a samostatne napájanie prierez podľa odberu a úbytku napätia vodičmi CYSY (2x2,5). Vodiče sa vedú oddelenou káblovou trasou od silových vedení inštalovaných v objekte.

4.2 Zahmlievacie zariadenie

V praxi sa začali používať taktiež systémy na ochranu objektov formou zahmlenia priestoru a so súčasným spustením sirény vzniká šok a znemožní priestorovú orientáciu páchateľa, ktoré zabránia páchateľovi spôsobiť väčšie škody. Taktiež ako sekundárny efekt zdržia páchateľa v objekte. Ide o efektívny novodobý nástroj zabezpečenia vnútorných priestorov objektov. Zariadenia nemajú negatívny vplyv na osoby a predmety.

Zdroj: PROTECT A/S, [online] http://www.protectglobal.com

Obrázok 15. Zahmlievacie zariadenia

Hypermarket navrhujeme zabezpečiť zahmlievacím systémom. Pre konkrétne priestory objektu navrhujeme zahmievací systém Protect 2200i, výrobca PROTECT A/S Denmark (obrázok č. 15). Ide o inovatívne zariadenie, ktoré produkuje 1100 – 2200 m3 hmly. Objem hmly je nastaviteľný. Jedna zahmlievacia náplň obsahuje 3l nádobu s kvapalinou, ktorá zabezpečí 6 zahmlení objektu. Potom je potrebné zahmlievaciu kvapalinu doplniť. Proti výpadku sieťového napájania navrhujeme zálohovanie systému záložnými olovennými AGM akumulátormi v počte 2 ks aku 12 V s kapacitou 1,2 Ah.

Zariadenie má zabudované 3 aktivačné a 2 ovládacie vstupy, ktorými po integrácii do PSN zabezpečíme zahmlenie objektu. V prípade aktivácie poplachového stavu sa poplachový výstup RZ PSN aktivuje a prenesie spúšťací impulz na vstup zahmlievacieho zariadenia, čím dôjde k jeho aktivácii. V prípade poruchového stavu alebo sabotáže zariadenia tieto sú signalizované na 3 výstupoch typu relé, ktoré spätne integrujeme do zabezpečovacieho systému a zabezpečíme signalizáciu týchto stavov obsluhe zariadenia.

V predmetnej aplikácii je potrebné umiestnenie mimo cesty k únikovým východom alebo požiarnych únikových trás. Inštaluje sa tak, aby bola vzdialenosť k najbližšiemu predmetu alebo povrchu minimálne 2,5 m. Taktiež jeho umiestnenie je potrebné mimo normálny dosah, napríklad pri podlahe, kde by mohol byť v dosahu detí alebo zvierat. Ak sú inštalované v priestoroch inštalácie s automatickými požiarnymi – hasiacimi systémami, sú potrebné špeciálne bezpečnostné opatrenia. Podobné opatrenia sú potrebné aj v bytových domoch.

4.3 Systém kontroly vstupu

Systém kontroly vstupu rieši oprávnenie pre konkrétne osoby na vstup do jednotlivých častí a oddelení objektu. Má priamy súvis s režimovými opatreniami v objekte. Varianty sú kartový systém, prívesky (obrázok č. 16), PIN alebo použitie biometrických údajov na jednoznačnú identifikáciu osôb – personálu v objekte.

Zdroj: ROGER sp.j., [online] http://www.roger.pl

Obrázok 16. Varianty transpondérov a príslušenstva

Pre predmetnú aplikáciu navrhujeme použitie systému RACS od výrobcu ROGER. Systém obsluhuje 4000 užívateľov zaradených do 250 skupín. V prípade potreby systém umožňuje ovládať aj výťahy max. do 32 poschodí. Je ponechaná dostatočná systémová rezerva na počet užívateľov, ktorí budú vstupovať do jednotlivých priestorov a ich zaradenie do skupín.

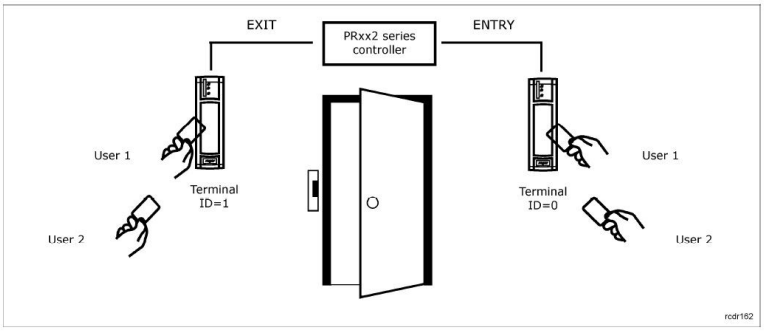
Ovládanie na bežné priechody Proximity kartou 125 kHz prostredníctvom čítačiek PRT-12LT. Pre vybrané miestnosti za účelom zabezpečenia komfortu navrhujeme čítačku biometrických údajov typu RFT1000 na snímanie otlačku prsta (obrázok č. 17). Predmetná čítačka sníma jednotlivé papily prsta, ktoré sú jedinečné u každého človeka a tým zaisťuje podľa ich umiestnenia jednoznačnú identifikáciu a overenie užívateľa.

Zdroj: ROGER sp.j., [online] http://www.roger.pl

Obrázok 17. Varianty čítačiek PRT-12LT a RFT1000

Čítačky komunikujú pomocou zbernice RS-232 a sú pripojené do riadiacej jednotky PR-402. Takýto set je vždy pre jedny dvere. Na jednotlivé dvere sa inštaluje prepúšťací elektrický zámok alebo prídržný magnet podľa typu dverí a ich požadovaného ovládania, resp. ovládanie garážových brán. Otvorenie dverí je kontrolované a v prípade otvorenia mimo impulzu systému vyvolá poplachový stav neoprávneného vstupu. Rovnako je kontrolovaný čas, po ktorý môžu byť otvorené dvere a po jeho prekročení je taktiež vyvolaný poplach. Princíp zapojenia čítačiek a ovládania dverí s činnosťou pri priechode dverami je zrejmý z obrázku č. 18.

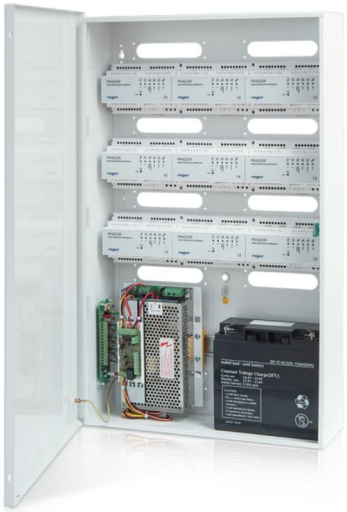
Pri ovládaní dverí je potrebné zabezpečiť únikové trasy v prípade požiaru a otvorenie únikových trás. Je to špecifické najmä v objektoch, kde sa vyskytuje viac osôb. Únikové trasy a únikové východy určuje požiarno evakulačný plán objektu.



Zdroj: ROGER sp.j., [online] http://www.roger.pl

Obrázok 18. Zapojenie čítačiek a ovládania dverí

Následne jednotka PR-402 prostredníctvom zbernice RS-485, ako jedna z max. 100 riadiacich jednotiek, môže komunikovať s modulom integrácie CPR-32 NET, ktorý udalosti preklápa do siete WAN/LAN. V predmetnej aplikácii však úplne bude postačovať prevodník UT-2USB, ktorý bude robiť prevod zo zbernice RS-485 na USB a bude pripojený do počítača s riadiacim software. Jednotlivé jednotky sa vyrábajú v dvoch verziách a to na zabudovanie do klasických plechových alebo plastových skriniek používaných napr. v zabezpečovacích zariadeniach – moduly sú iba osadené dosky plošných spojov alebo moduly určené na montáž na DIN lištu do rozvádzača. Variantu s modulmi na DIN lištu preferujeme. Ukážka rozvádzača z inštalácie prístupového systému s modulmi v prevedení určenom na DIN lištu sa nachádza na obrázku č. 19. Pri takomto vyhotovení inštalácie je potrebné zabudovať do rozvádzača sabotážny kontakt vyvedený do zabezpečovacieho systému. Originálne, výrobcom dodávané skrinky na moduly v štandardnom doskovom prevedení už obsahujú sabotážny kontakt a preto nie je potrebné jeho doplnenie v prípade takéhoto variantu prevedenia riadiacich systémov. Pri inštalácii jednotlivých systémov je potrebné vziať do úvahy maximálnu vzdialenosť navrhnutých čítačiek od riadiacej jednotky s ohľadom na použitú zbernicu komunikácie RS-232 a umiestniť riadiace jednotky decentrálne. V prípade požiadavky na centrálne umiestnenie prvkov sú k dispozícii aj čítačky už priamo s integrovaným modulom rozhrania RS-485, ktoré sa potom môžu ovládať prostredníctvom centrálne umiestnených jednotlivých modulov systému.

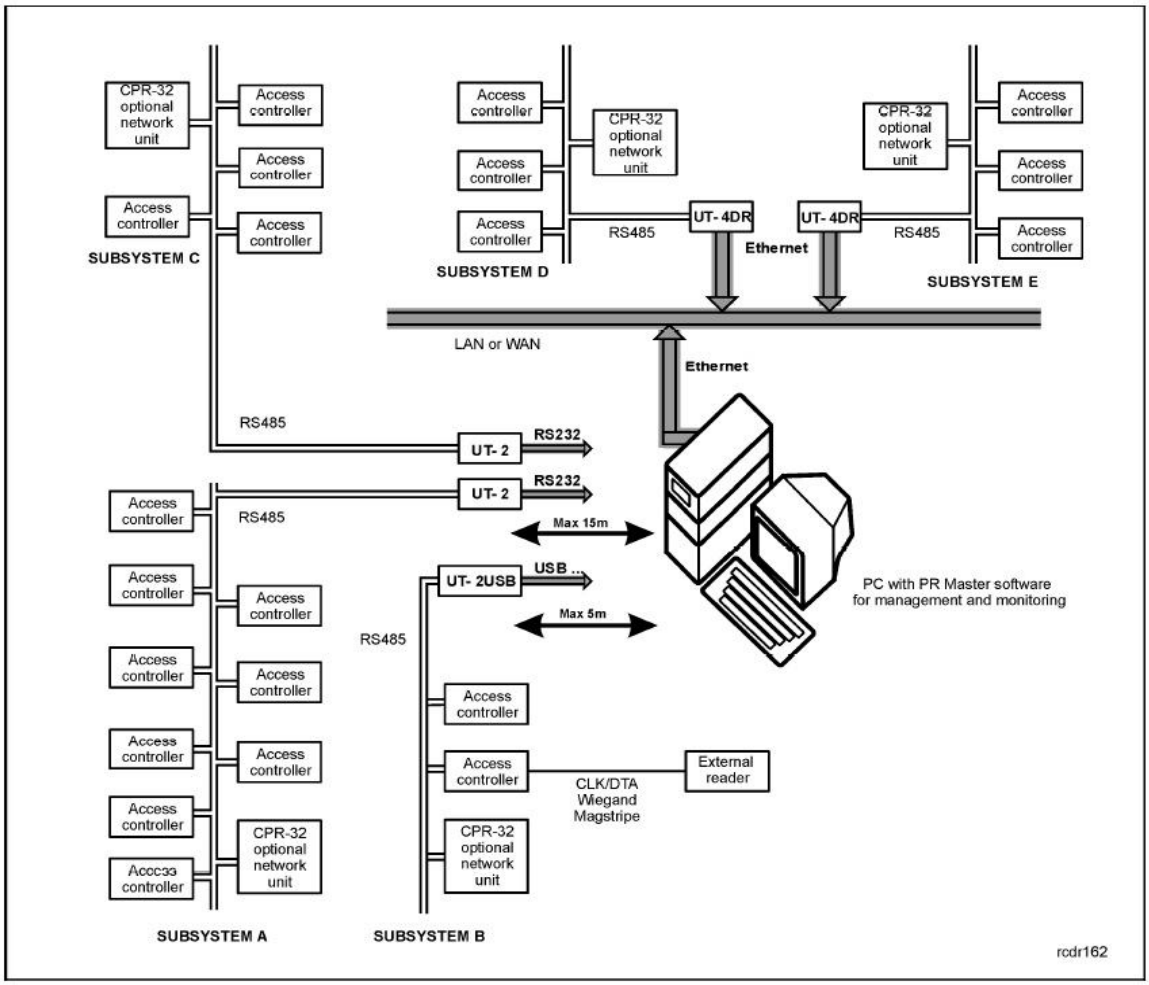


Zdroj: ROGER sp.j., [online] http://www.roger.pl

Obrázok 19. Rozvádzač s modulmi v prevedení DIN

Voliteľne je možná aj nadstavba systému na dochádzkový systém jednoduchým doplnením čítačky pre dochádzku s príslušným obslužným software. Riadiaci software systému je PR-MASTER. Software umožňuje editovať užívateľov, priraďovať im oprávnenia vstupu do jednotlivých priestorov, nastavovať evakuačné zóny a sledovať príchody/odchody a prítomnosť osôb v priestoroch a častiach objektu.

V prípade rozsiahlych objektov je možné naplno využiť možnosti systému. Hardwarové limity sú nastavené tak vysoko, že sú prakticky bez obmedzenia. Rozsah a možnosti systému sú zjavné z obrázku č. 20, kde je načrtnutá úplná štruktúra a jeho možnosti. Jednotlivé subsystémy na obrázku zobrazujú možnosti rôznych druhov pripojenia a štrukturovania riadiacich jednotiek a čítačiek, kde vo variante Subsystem B je rozhranie vetvy systému tvorené prevodníkom zbernice RS-485 na USB port – tu je vzdialenosť posledného bodu vetvy limitovaná maximálnou garantovanou vzialenosťou 5 m USB kábla, vo variantách Subsystem A,C je situácia obdobná, len s rozhraním RS-485 na RS-232 so vzdialenosťou sériového kábla maximálne 15 m, u variánt Subsystem D, E je rozhranie tvorené prevodníkom zo zbernice RS-485 na TCP/IP. Táto varianta je vhodná na rozsiahle alebo vzdialené aplikácie.



Zdroj: ROGER sp.j., [online] http://www.roger.pl

Obrázok 20. Štruktúra prístupového systému

Zbernica RS-485 sa zapája do línie, hviezdy, stromu a je dovolené akékoľvek vetvenie tejto zbernice. Zapojenie do kruhu (loop – slučka) nie je prípustné. Prvky na zbernici môžu byť adresovateľné od č. 00 do č. 99. Vzdialenosť zbernice je max. do 1200 m. Zbernica je vedená jedným párom krúteného vodiča. Výrobca doporučuje použitie netieneného UTP kábla cat. 5 (resp. cat. 6), ale v praxi sa najčastejšie používa kábel JYSTY 2x2x0,8, kde zostáva jeden pár ako rezerva alebo sa používa na napájanie zariadení. U väčšieho rozsahu inštalácie sa napájanie vedie samostatným vedením alebo sa realizuje decentralizovane. V prípade centralizovaného napájania sa vodiče dimenzujú podľa odberu zariadení s prihliadnutím na úbytok napätia vplyvom prierezu a vzdialeností.

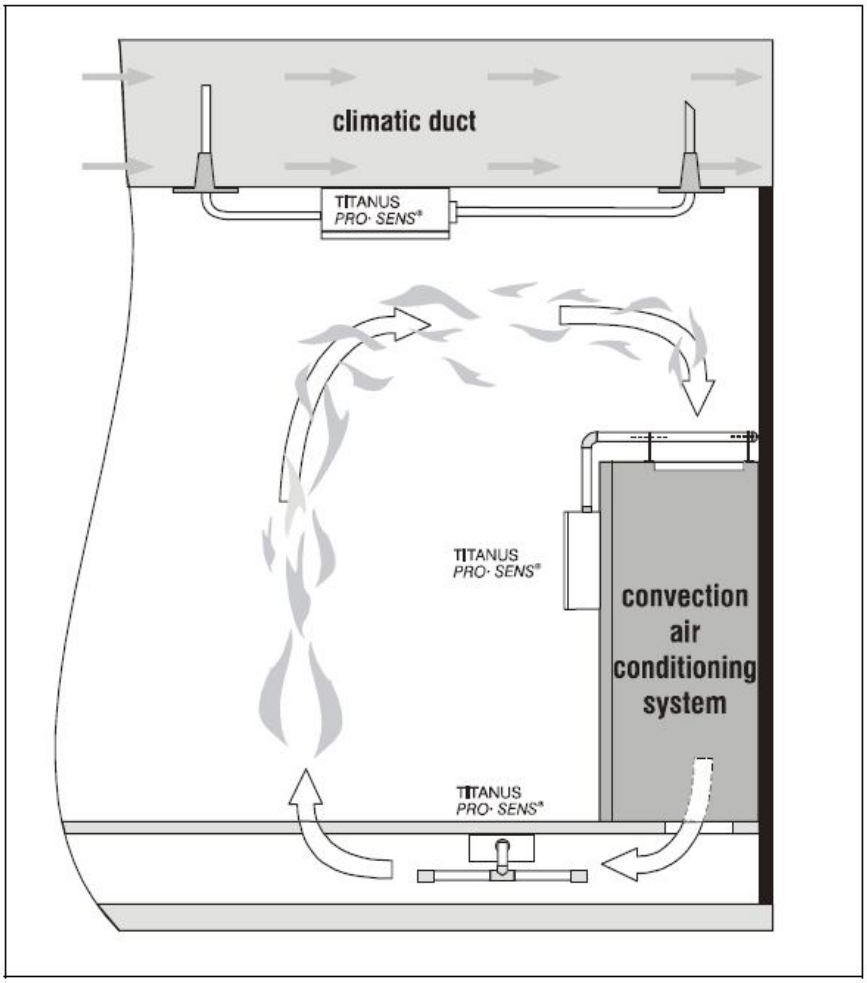
4.4 Elektrická požiarna signalizácia

Keďže ide o členité miestnosti navrhujeme využiť na detekciu požiaru nasávací systém, ktorý detekuje požiar z odsávaného vzduchu z jednotlivých miestností. Vzduch z týchto miestností sa zberným potrubím vzduchotechniky nasáva do modulu detektora. Navrhujeme použitie systému TITANUS PRO. Ako riadiacu jednotku navrhujeme použitie typ TP1A z produkcie LABOR STRAUSS Sicherungsanlagenbau GmbH s modulom detektora nasávacieho systému typ DM-TP-10L od toho istého výrobcu (obrázok č. 21). Modul vyhodnocuje stav požiaru a pomocou výstupných kontaktov zariadenia je možná signalizácia stavu požiaru, poruchy, externá indikácia a reset poplachu. Týmto spôsobom je možná aj integrácia systému.

Zdroj: Alarm und Sicherungsysteme GmbH, [online] http://www.wagner.de

Obrázok 21. Riadiaca jednotka a detektor TITANUS PRO

Princíp činnosti a dopojenia nasávacieho detekčného systému do vzduchotechniky je na obrázku č. 22. Štandardná vzduchotechnika v objekte dodáva v zmysle platných noriem do objektu čerstvý vzduch a z miestností odvádza vyčerpaný vzduch, ktorý práve detekujeme na prítomnosť dymu a následne požiaru. Bližšie popisy k spôsobu vedenia potrubí, ich prepojeniu, spôsob napojenia na potrubia vzduchotechniky a ostatné technické podmienky sú detailne popísané v servisnej dokumentácii výrobcu.



Zdroj: Alarm und Sicherungsysteme GmbH, Manuál technika

Obrázok 22. Princíp činnosti TITANUS PRO

4.5 Priemyselná televízia

Systémy priemyselnej televízie umožňujú snímať, monitorovať, zobrazovať, archivovať obraz (príp. aj zvuk) v zabezpečenom objekte a prenášať ho do miestnosti obsluhy alebo na jej vzdialené stanovisko, napr. SRP. Okrem monitoringu aktuálnej situácie poskytujú vyhodnotenie neštandardného stavu a zaznamenávaním dát umožňujú poskytnúť objasnenie situácie a dôkazový materiál. U systémov priemyselnej televízie je určujúca kvalita detailov obrazu. Z tohoto dôvodu je nevyhnutné stanoviť požadovanú mieru detailov snímaného a zaznamenávaného obrazu a na základe toho navrhnúť vhodné riešenie, ktoré takúto kvalitu poskytuje. Na základe východiskovej požadovanej kvality detailov obrazu sa následne navrhujú také komponenty kamerového systému, ktoré

zodpovedajú požiadavkám užívateľa systému. Aj keď sú inovácie v tejto oblasti v poslednom období veľmi progresívne, najlepšie je navrhnúť a inštalovať zariadenia v takej kvalite, ktorá bude zodpovedať požiadavkám a nebude potrebné zariadenia v kratšom či dlhšom časovom horizonte meniť.

Na základe analýzy a potrieb zabezpečenia konkrétneho objektu navrhujeme použitie systémov od výrobcu AV TECH corp., ktoré nám svojim širokým portfoliom produktov poskytnú komplexné riešenie zabezpečenia objektu s akceptovaním špecifík jednotlivých priestorov. V predajných priestoroch a vonkajších priestoroch navrhujeme použitie otočné speed dome kamery z produkcie tohoto výrobcu typu AVM-583 (obrázok č. 23). Kamera má Full HD rozlíšenie s technológiou WDR – 1920 x 1080 – 1080 pix. pri 25 fps., kompresia H.264 / MJPEG, citlivosť 0,1 lux, optický zoom 20x, digitálny 16x, objektív 4,7 – 94 mm, PTZ so 16 programovateľnými pozíciami, sekvencie 4 obchôdzky so 16 predprogramovanými pozíciami, ONVIF, Half duplex audio – obojsmerné eterný vstup aj výstup, rozhranie TCP/IP s PoE (IEEE 802.3af) – 11,5W, pri napájaní DC 12V 9,6 W, krytie IP-66.

Zdroj: AVTECH Corp., [online] http://www.avtech.com.tw

Obrázok 23. Kamera AVM-583

Stacionárne kamery navrhujeme použiť typu AVM-561 od AVTECH Corp. (obrázok č. 24). Predmetná kamera má Full HD rozlíšenie s technológiou WDR – 1920 x 1080 – 1080 pix. pri 25 fps., kompresia H.264 / MJPEG, citlivosť 0,1 lux, 0 lux s IR, optický motor zoom, objektív 5 - 50 mm, IR 50 m so zapnutou funkciou enhanced mode IR 70 m, rozhranie TCP/IP s PoE (IEEE 802.3af) – 14 W vrátane IR, krytie IP-67.

Zdroj: AVTECH Corp., [online] http://www.avtech.com.tw

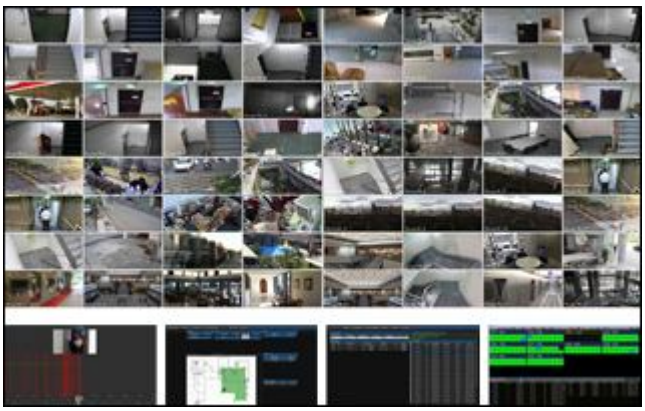
Obrázok 24. Kamera AVM-561

Záznamové zariadenie NVR AVH-516 (obrázok č. 25) podporuje až 16 kanálov v rozlíšení Full HD real time. Kamery sú pripojené prostredníctvom siete TCP/IP na vstup NVR 1 x GB a zaznamenávajú sa na max. 3 HDD o veľkosti 4 TB, rozlíšenie záznamu 1920 x 1080 – 1080 pix. pri 30 fps vo formáte H.264, možnosť externého zálohovania na eSATA disky, USB. Podpora vonkajšieho pripojenia cez LAN z iPhone, iPad, Android, Eagle Eyes, Video viewer (WIN) alebo Internet explorera. Výstup lokálne HDMI vo Full HD rozlíšení. Nahrávacie módy: manuálny, časový, detekcia pohybu alebo alarmový. Pri alarmovom nahrávaní je možný záznam aj časového úseku pred poplachom. Zariadenie obsahuje samostatný LAN vstup na kamery a Internet výstup na WAN, čo zabezpečuje hardwarový fireval pre kamery. Na integráciu má zariadenie k dispozícii vstupy aj výstupy.

Zdroj: AVTECH Corp., [online] http://www.avtech.com.tw

Obrázok 25. NVR AVH-516

Software TRIDENT dokáže integrovať až 64 kanálov pre centrálnu správu zariadení od výrobcu AVTECH Corp. (obrázok č. 26). Jedná sa o centrálnu monitorovaciu stanicu, kde je možné prostredníctvom TCP/IP pripojiť nielen jednotlivé kamery, ale aj priamo NVR, kde vznikne už naozaj rozsiahly systém dostatočne pokrývajúci potreby ľubovoľného hypermarketu.



Zdroj: AVTECH Corp., [online] http://www.avtech.com.tw

Obrázok 26. Software Trident

4.6 Integrácia jednotlivých podsystémov

Integrovaný poplachový systém je systém, ktorý má viac spoločných zariadení, z ktorých aspoň jedno je poplachová aplikácia [1]. V našom prípade ide o kombináciu jedntlivých poplachových systémov do jedného celku s vytvorením väzieb na sekundárne nepoplachové systémy, čím rozumieme systém automatizácie budovy, systém vzduchotechniky, klimatizáciu, vykurovanie (MaR), osvetlenie apod. Keďže návrh riešenia je tvorený samostatnými decentralizovanými systémami, funkčnosť týchto jednotlivých samostatných systémov nie je ovplyvňovaná prípadnou poruchou iného systému, čím sa vytvorila veľká spoľahlivosť a boli vyriešené otázky redudancií informačných kanálov, nakoľko funkčnosť jednotlivých dielčích systémov je nezávislá na prevádzke hlavného riadiaceho systému a je možné ich ovládať aj samostatne bez neho, napr. pri poruche integračného prvku.

Integráciou jednotlivých systémov od rôznych výrobcov, ktoré využívajú rôzne technológie a princípy činnosti, do väčšieho celku získame účinné efektívne riadenie a monitorovanie jednotlivých systémov, ktoré sa budú chovať ako jeden celok, čím sa napríklad pri zmene oprávnení jednotlivého užívateľa prenesie do všetkých podsystémov naraz (napr. do PSN a zároveň do SKV) a nie sú potrebné zmeny vo viacerých nezávislých programoch so samostatnou obsluhou a na inom princípe funkčnosti. Centralizovaná obsluha všetkých systémov teda prináša prehľadnosť, jednoduchosť a zvýšený komfort riadenia, ovládania a v špecifických prípadoch aj obsluhy zariadení. Okrem úspory energií a zvýšení bezpečnosti prinášajú aj flexibilitu pri rôznych zmenách, napr. pri zmene dispozícií priestorov, univerzálnosť riešenia a komplexné riešenie všetkých požiadaviek užívateľa objektu.

Jednoznačne dochádza k zvýšeniu pridanej hodnoty v porovnaní so samostatne funkčnými systémami nie len pre majiteľa objektu, ale tiež pre SBS. Integrácia systémov prináša konštantnú stabilitu ochrany objektu. Integrovanie bezpečnostných systémov prináša zákazníkovi vo svojej podstate minimalizáciu počtov pracovníkov ostrahy objektu.

Na integráciu jednotlivých systémov do vyššieho celku navrhujeme použitie integračného software C4, ktorý poskytuje centralizované, viacužívateľské technologické a grafické rozhranie na spravovanie bezpečnosti budov. C4 poskytuje jednotné softwarové riešenie, ktoré sa dokáže prispôsobiť konkrétnym požiadavkám malých aj veľkých inštalácií a integruje všetky bezpečnostné technológie do jedného unifikovaného inteligentného rozhrania. C4 teda integruje rôzne bezpečnostné systémy od rôznych

1 CLC/TS 50398:2008

výrobcov do jediného centrálneho riešenia riadenia, ovládania a monitoringu systémov. Poskytuje centrálnu správu bezpečnostných riešení, vizualizáciu a monitoring zariadení, automatizáciu bezpečnostných procesov, analýzu a vyhodnocovanie bezpečnostných informácií, centrálny manažment osôb a identifikátorov a podporu krízového manažmentu.

Riešenie C4 pokrýva komplexné riešenie integrácie všetkých nami navrhnutých systémov zabezpečenia objektu pokrývajúce softwarové riešenie aj moduly hardwarovej integrácie jednotlivých systémov do systému C4.

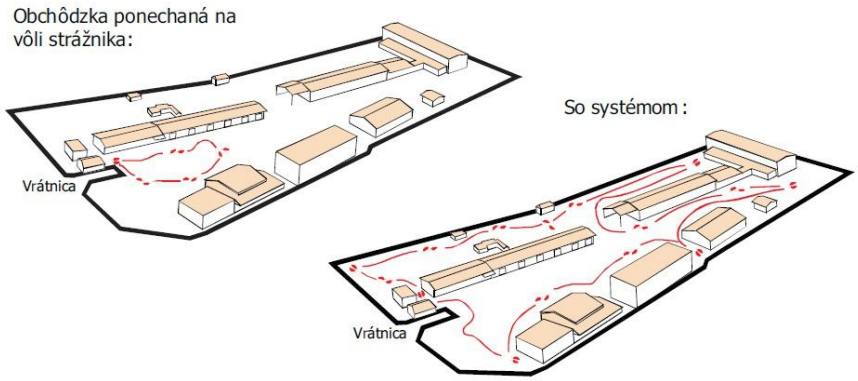
Zdroj: Gamanet a.s., [online] http://www.c4portal.com

Obrázok 27. Integračný software C4

4.7 Obchôdzkový systém

Obchôdzkový systém je manažérsky systém určený na plánovanie, evidenciu a následnú kontrolu činnosti zamestnancov fyzickej ostrahy objektu vrátane ich identifikácie pri pravidelných alebo nepravidelných ohliadkach objektu. Správne navrhnutý systém vyhodnocuje správnosť vykonania ohliadok objektu, vykazuje rozdiely voči štandardne navrhnutým postupom, harmonogramom a časom obchôdzok, ich rozsahu a poskytuje výstupy v textovej a grafickej podobe so zvýraznením nesúladov. Na stanovených trasách sú rozmiestnené kontrolné body, ktoré pracovník SBS sníma počas ohliadky objektu. Môže byť definovaná časová postupnosť viacerých okruhov ohliadky, čím sa stanovujú trasy obchôdzok vrátane časového priebehu. Tieto sa môžu meniť na základe jednotlivých dní podľa vopred stanoveného algoritmu.

Porovnanie kvality obchôdzok pred zavedením obchôdzkového systému a po jeho zavedení je na obrázku č. 17. Z obrázku je zreteľný rozdiel v kvalite vykonávania ostrahy strážnou službou SBS po zavedení kontrolného mechanizmu.



Zdroj: vlastné spracovanie

Obrázok 28. Porovnanie obchôdzok pred a po zavedení systému

Navrhujeme použitie systému Patrol II z produkcie Roger. Systém pracuje na princípe bezkontaktného snímania kontrolných bodov počas ohliadky objektu pracovníkom SBS čítačkou. Údaje z RFID kontrolných bodov typov PK-3 alebo PK-2 sa ukladajú do čítačky typ Patrol II LCD. Čítačka má kapacitu 32.768 udalostí, pričom eviduje dátum, čas, názov kontrolných bodov, osobného identifikátora pracovníka. LCD displej je podsvietením, čo je praktické v noci alebo v miestach so slabým osvetlením. Všetka činnosť sa vykonáva stlačením jediného tlačítka, z tohoto dôvodu je obsluha zariadenia veľmi jednoduchá. Kapacita akumulátora vydrží na 8.000 načítaní kontrolných bodov. Akumulátor čítačky sa nabíja prostredníctvom USB portu alebo samostatného adaptéra. Udalosti zaznamenané v čítačke nie je možné žiadnou manipuláciou s čítačkou navymazať. Následne po pripojení k počítaču prostredníctvom portu USB sú zaznamenané udalosti stiahnuté do nadstavbového software za účelom ďalšieho spracovania, vyhodnotenia a tlače, čím je k dispozícii manažérsky nástroj na zabepečenie zvýšenej bezpečnosti objektu formou neustálej kontroly činnosti ostrahy objektu pri obchôdzkach.

Zdroj: ROGER sp.j., [online] http://www.roger.pl

Obrázok 29. Čítačka systému Patrol II.

Bezkontaktné kontrolné body pracujú podľa štandardu EM 125 kHz. Sú vo vyhotovení do vnútorného prostredia – typ PK-2 a do vonkajšieho prostredia – typ PK-3 (obrázok č. 19). Nie je potrebné ich napájanie a z tohoto dôvodu je montáž, inštalácia a ich implementácia veľmi jednoduchá. Kontrolné body sa pripevňujú skrutkami prípadne nalepením. Umiestňujú sa na kontrolných stanoviskách v objekte, ktorými musí pracovník ostrahy prejsť. Taktiež sú minimálne požiadavky na údržbu.

Zdroj: ROGER sp.j., [online] http://www.roger.pl

Obrázok 30. Kontrolný bod PK-2 a PK-3

ZÁVER

V práci sme sa venovali návrhu elekrického zabezpečenia budovy supermarketu a perimetra za účelom ochrany budovy a pozemkov v jej okolí s ohľadom na kvalitu zabezpečenia. Na základe analýzy rizika a nebezpečenstiev sme za použitia dostupných technických prostriedkov na trhu vytvorili komplexný návrh riešenia zabezpečenia objektu a jeho perimetra. Vytvorením komplexného účelného systému manažmentu rizika skladajúceho sa z prostriedkov mechanického, technického a režimového zabezpečenia sme vzájomne cielene logicky prepojili samostatné prvky do jedného integrovaného logického funkčného celku systému zabezpečenia, čím vznikol homogénny systém zabezpečujúci maximálnu mieru bezpečnosti objektu s vysokou sofistifikovanosťou a jednoduchou obsluhou. Integrovaním jednotlivých decentralizovaných zariadení sme vytvorili jeden vysoko účinný centralizovaný systém. Účinným prepojením preventívnych a technických opatrení v objekte sa minimalizujú riziká s cieľom na odstránenie alebo elimináciu rizík.

Cieľom diplomovej práce bolo vytvorenie literatúrneho prieskumu z oblasti jednotlivých stupňov zabezpečenia objektov a pozemkov, popísať jednotlivé technológie a spôsob ich použitia, na základe výstupov vytvoriť projekt elektrického zabezpečenia objektov a pozemkov v jeho okolí s ohľadom na kvalitu. Na základe vytýčených cieľov diplomovej práce boli identifikované jednotlivé druhy rizík a popísané požiadavky na manažment rizika s bližším popísaním bezpečnostných rizík a technických prostriedkov používaných na ochranu objektu. Jednotlivé používané technológie boli prenesené na konkrétne prvky komponentov technickej ochrany objektu a boli navrhnuté jednotlivé poplachové systémy, ktoré riešia všetky relevantné otázky zabezpečenia objektu a jeho okolia s prihliadnutím na kvalitu zabezpečenia objektu a s rešpektovaním špecifík hypermarketu. Bol navrhnutý koncept technickej ochrany objektu s konkrétnymi návrhmi systémov až do úrovne komponentov – detektorov, senzorov, riadiacich a indikačných zariadení a bola popísaná ich funkčnosť a spôsob použitia, pričom komponenty boli navrnuté s prihliadnutím na kvalitu zabezpečenia. Celková úroveň kvality zabezpečenia a komfortu obsluhy sa zvýšila na najvyššiu možnú mieru integráciou jednotlivých dielčích samostatných systémov integračným systémom, ktorý poskytuje jednoduchú, intuitívnu a spoľahlivú integračnú platformu na jednotný centralizovaný spôsob obsluhy jednotlivých zariadení. V prípade ľubovoľnej poruchy alebo iného neštandardného stavu v systéme bola ponechaná možnosť decentralizovaného ovládania jednotlivých samostatných systémov,

čím sa vylúčila možnosť, že porucha niektorého dielčieho systému by mohla ovplyvniť funkčnosť ktoréhokoľvek iného poplachového subsystému a ohroziť tým technickú ochranu ako celku. Navrhnuté jednotlivé subsystémy sa kvalitou zaraďujú medzi technologickú špičku tejto doby a vyrábajú ich renomovaní svetoví výrobcovia zabezpečovacej techniky s mnohoročnými skúsenosťami overenými v praxi. Cieľ diplomovej práce sa podarilo splniť vo všetkých požadovaných bodoch.

ZOZNAM POUŽITEJ LITERATÚRY

Knihy:

[1.] ANDERSEN, T.J. - SCHRODER, P.W. 2010. Strategic Risk Management Praktice, In *Cambridge University Press*, Cambridge, 2010. ISBN: 978-0-521-11424-0

[2.] BATE, N. 2009. *Ako poraziť recesiu – Plán na prežitie v podnikaní.* Bratislava: Eastone Group, 2009. ISBN 978-80-8109-088-2

[3.] COOPER, F. - GREY, S. - RAYMOND, G. - WALKER, P. 2004. *Project Risk Management Guidelines: Manage Risk in Large Projects and Complex Procurements.* 1st ed. Chichester, U.K.: Wiley, 2004. ISBN: 0-470-02281-7

[4.] FILIP, S. - ŠIMÁK, L. - KOVÁČ, M. 2011. *Manažment rizika.* Bratislava: Sprint dva, 2011. ISBN: 978-80-89393-49-7

[5.] FOTR, J. - SOUČEK, I. 2005. *Podnikatelský záměr a investiční rozhodování.* Praha: Grada publishing, 2005. ISBN: 80-247-0939-2

[6.] GAŠPIERIK, L. 2010. *Prevencia kriminality a inej protispoločenskej činnosti.* Žilina: Multiprint s.r.o., 2010. ISBN 978-80-970410-0-7

[7.] GOZORA, V. 2002. *Krízový manažment.* Nitra: SPU Nitra, 2000. ISBN: 80-7137-802-X

[8.] KANDRÁČ, J. - SKARBA, D. 2000. *Metodický postup na hodnotenie rizík nebezpečných prevádzok a štúdia o podnikoch v SR.* Bratislava: RISK consult, 2000, bez ISBN

[9.] KAPLAN, R.S. 2008. Enterprise Risk Management In *The Centennial Global Business Summit*, Harward Business School, 2008. bez ISBN

[10.] KORECKÝ, M. - TRKOVSKÝ, V. 2011. *Management rizik projektú.* Praha: Grada Publishing, 2011. ISBN: 978-80-247-3221-3

[11.] KOTLER, P. - WONG, V. - SAUNDERS, J. - ARMSSTRONG, G. 2007. *Moderní marketing.* Praha: Grada Publishing, 2007. ISBN 978-80-247-1545-2

[12.] KULAŠÍK, P. a kol. 2002. *Slovník bezpečnostných vzťahov*. Bratislava: Smaragd, 2002. ISBN: 80-89063-08-X

[13.] KORECKÝ, M. - TRKOVSKÝ, V. 2011. *Management rizik projektú – se zaměřením na projekty v prúmyslových podnicích.* Praha: Grada publishing, 2011. ISBN: 978-80- 247-3221-3

[14.] KŘEČEK, S. a kol. 2006. *Příručka zabezpečovací techniky*. Blatná: Cricetus, 2006.

ISBN: 80-902938-2-4

[15.] LOVEČEK, T. - NAGY, P. 2008. *Bezpečnostné systémy – Kamerové bezpečnostné systémy.* Žilina: EDIS – vydavateľstvo ŽU, 2008. ISBN: 978-80-8070-891-1

[16.] NOVÁK, L. a kol. 2010. *Plánovanie zdrojov na riešenie krízových situácií.* Bratislava: Crr.sk, 2010. ISBN: 978-80-970272-4-7

[17.] OGC: *Management of Risk: Guidance for Practitioners*, OGC: *The Stationery Office*, Londýn, 2007, ISBN: 978-0-11-331038-8

[18.] TOFFLER, A. - TOFFLEROVÁ, H. 2002. *Válka a antiválka. Jak porozumět dnešnímu globálnímu chaosu.* Praha: Dokořán a Argo, 2002. ISBN 80-86569-160

[19.] STRAUS, J. 2007. *Kriminalistická technika.* Plzeň: Aleš Čeňek, 2. rozšírené vydanie, 2007. ISBN: 978-80-7380-052-9

[20.] VALOUCH, J. 2012. *Projektování bezpečnostních systémů.* [skriptum]. Zlín: UTB, 2012. ISBN 978-80-7454-230-5

[21.] VALOUCH, J. 2012 Techniques of Integration of Alarm Systems. *In TRANSACTIONS of the VŠB - Technical University of Ostrava.* Ostrava: VŠB, 2012. No. 1, Vol. VII. Safety Engineering Series. *ISSN: 1801-1764*

[22.] VARCHOVÁ, T. - DUBOVICKÁ, L. 2008. *Nový manažment rizika.* Bratislava: IURA Edition, 2008. ISBN: 978-80-8078-171-0

Normy:

[23.] AS/NZS 4360:2004: Risk Management Guidelines, Companion to AS/NZS 4360:2004. Sydney, Welington: Standards Australia, ISBN: 0-7337-5960-2

[24.] AS/NZS 4360:2004: Risk Management, 3rd ed., New Zealand: Standards Australia, ISBN: 0-7337-5904-1

[25.] BS/IEC 2198:2001: Project Risk Management – Application Guidelines, London, U.K.: British Standards Institute, ISBN: 0-580-390195

[26.] BSI, IEC, ISO Guide 73:2002. Risk Management – Vocabundary – Guidelines for use in Standards BSI PD ISO/IEC, 1st ed. London, U.K.: British Standards Institute, ISBN: 0-580-40178-2

[27.] COSO ERM - Enterprise-wide Risk management, 2004, bez ISBN

[28.] ČSN EN 31010:2011: Management rizik – Techniky posuzování rizik. Český normalizační institut, bez ISBN

[29.] IEC/ISO 31010:2009: Risk management – Risk assessment techniques, 1st ed. Geneva, ISBN: 2-8318-5734-1

[30.] IRM/ALARM/AIRMIC: A Risk Management Standard, London 2002, bez ISBN

[31.] ISO 31000:2009: Manažment rizika – princípy a smernice, bez ISBN

[32.] ISO/IEC 3101:2009: Manažment rizika - hodnotenie rizík, bez ISBN

[33.] ISO Guide 73:2009: slovník, bez ISBN

[34.] Risk Management Standard - The Institute of Risk Management 2002, bez ISBN

[35.] STN 010380:2003: Manažérstvo rizika, bez ISBN

[36.] STN CLC/TS 50398:2009: Poplachové systémy – Kombinované a integrované poplachové systémy (STN 334597), bez ISBN

[37.] STN EN 50130:2003: Poplachové systémy, bez ISBN

[38.] STN EN 50131:2007: Poplachové systémy – Elektrické zabezpečovacie a tiesňové poplachové systémy, bez ISBN

[39.] STN EN 50132:2007: Poplachové systémy – Sledovacie systémy CCTV na používanie v bezpečnostných aplikáciách, bez ISBN

[40.] STN EN 61000:2009 – Elektromagnetická kompatibilita (EMC), bez ISBN

Zákony a vyhlášky:

[41.] Zákon NR SR č. 8/2009 Z.z. o cestnej premávke

[42.] Zákon NR SR č. 42/1994 Z.z. o civilnej ochrane obyvateľstva

[43.] Zákon NR SR č. 124/2006 Z.z. o bezpečnosti a ochrane zdravia pri práci

[44.] Zákon NR SR č. 129/2002 Z.z. o integrovanom záchrannom systéme

[45.] Zákon NR SR č. 152/1995 Z.z. o potravinách

[46.] Zákon NR SR č. 241/2002 Z.z. o ochrane utajovaných skutočností

[47.] Zákon NR SR č. 261/2002 Z.z. o prevencii závažných priemyselných havárií

[48.] Zákon NR SR č. 264/1999 Z.z. o technických požiadavkách na výrobky a o posudzovaní zhody

[49.] Zákon NR SR č. 314/2001 Z.z. o ochrane pred požiarmi

[50.] Zákon NR SR č. 355/2007 Z.z. o ochrane, podpore a rozvoji verejného zdravia

[51.] Zákon NR SR č. 428/2002 Z.z. o ochrane osobných údajov

Elektronické zdroje:

[52.] Internetové stránky WebFinance, Inc. [online] http://www.businessdictionary.com

[53.] Internetové stránky Committee of Sponzoring Organisations of the Treadway Commision [online] http://www.coso.org

[54.] Internetové stránky Disk Forensics Project: Center for Research on Computation

and Society @ Harvard University [online] http://www.eecs.harvard.edu/forensics/

[55.] Internetové stránky Forensics Project [online] http://www.simson.net

[56.] Internetové stránky Gamanet a.s. [online] http://www.gamanet.com a http://www.c4portal.com

[57.] Internetové stránky Oxford University Press [online] http://oxforddictionaries.com

[58.] Internetové stránky Honeywell [online] http://www.security.honeywell.com/

[59.] Internetové stránky Security revue [online] http://www.securityrevue.com, ISSN: 1336-9717

Interné a servisné materiály:

[60.] ABASYS SK, Avermedia, AVTECH, BOSCH, CGC, Ekey biometric systems, Honeywell, Labor Strauss, PROTECT, RISCO, ROEL, ROGER, SATEL, SENTROL, SIEMENS, VAGNER, VISONIC, XTRALIS

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

AGM	olovenné záložné akumulátory (Absorbed Glass mat)
CCA	analýza príčin následkov (Cause Consequence Analysis)
CLA	analýza pomocou kontrolných záznamov (Check List Analysis)
DVR	digitálny záznamník videosignálu (Digital Video Recorder)
EMC	elektromagnetická kompatibilita (Electromagnetic Compatibility)
EPS	elektrická požiarna signalizácia
FTA	analýza stromom porúch (Fault Three Analysis)
FULL HD	rozlíšenie 1080 riadkov, každý 1920 bodov – 1920x1080 pixelov
HAZAN	analýza nebezpečenstva (Hazard Analysis)
HD	vysoké rozlíšenie (High Definition)
HD READY	rozlíšenie 720 riadkov, každý riadok 1280 bodov – 1280x720 pixelov
HDD	Pevný disk (Hard Disk)
HDMI	rozhranie vo vysokom rozlíšení (High Definition Multimedia Interface)
HRA	analýza spoľahlivosti človeka (Human Reliability Analysis)
HTA	analýza stromom nebezpečenstva (Hazard Three Analysis)
IZ	indikačné zariadenie - klávesnica
IBS	integrovaný bezpečnostný systém
IP	jednoznačné sieťové rozhranie v počítačovej sieti (Internet Protocol)
LAN	lokálna počítačová sieť, intranet (Local Area Network)
LCD	zobrazovacia jednotka z tekutých kryštálov (Liquid Crystal Displays)
MPX	megapixelový obraz – obraz s vysokým rozlíšením
NVR	sieťový záznamník videosignálu (Network Video Recorder)
PC	počítač alebo notebook
PSN	poplachový systém na hlásenie narušenia
PTV	priemyselná televízia
PIN	osobné identifikačné číslo (Personal Identification Number)
PIR	infrapasívny detektor (Pasiv Infra Red detector)
RR	rýchle hodnotenie (Rapid Ranking)
RT	rutinné testy (Routine Tests)
RZ	riadiace zariadenie - ústredňa
SA	bezpečnostný audit (Safety audit)
SKV	systém kontroly vstupu
SRP	stredisko registrácie poplachov
TCP	protokol riadenia prenosu, jadro prenosu v sieti internet

VRLA	ventilom riadené kyselinové akumulátory (Valve Regulated Lead Acid)
WAN	vonkajšia počítačová sieť, napr. internet (Wide Area Network)

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK