

Návrh bezpečnostní politiky ve vybrané společnosti

The security policy draft in selected company.

Bc. Lucia Procházková



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Lucia Ďuricová**
Osobní číslo: **A13706**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **kombinovaná**

Téma práce: **Návrh bezpečnostní politiky ve vybrané společnosti**
Téma anglicky: **A Proposed Security Policy for a Selected Company**

Zásady pro vypracování:

1. Proveďte analýzu současného stavu z pohledu řešeného problému.
2. Vypracujte návrh řízení vybraných bezpečnostních rizik ve vybrané společnosti.
3. Navrhněte strukturu bezpečnostní politiky ve vybrané společnosti.
4. Aplikujte zásady a struktury v rámci vybrané společnosti.
5. Analyzujte aplikovatelnost bezpečnostní politiky a její přínos.



Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. LÁTAL, I., ŠTAJNERSKÝ, M.: Bezpečnostní zásady ochrany podniku: prevence a řešení krizových situací, 4. vydání, Praha: PROSPEKTUM, 2001, 120 str., ISBN 80-7175-091-3.
2. BRABEC, F. a kol.: Bezpečnost pro firmu, úřad, občana, 1. vydání, Praha: Public History, 2001, 400 str., ISBN 80-86455-04-06.
3. KAMENÍK, J., BRABEC, F. a kol.: Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur, 1. vydání, Praha: ASPI, a.s., 2007, 340 str., ISBN 978-80-7357-309-6.
4. LAUCKÝ, V.: Technologie komerční bezpečnosti II, 1. vydání, Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 123 str., ISBN 80-7318-231-9.
5. LUKÁŠ, Luděk a KOLEKTIV. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VerBuM, 2011, 316 s. ISBN 978-80-87500-05-7.
6. BRABEC, F.: Ochrana bezpečnosti podniku, 1. vydání, Praha: EUROUNION, 1996, 204 str., ISBN 80-85858-29-0.

Vedoucí diplomové práce:

Ing. Martin Hromada, Ph.D.

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

7. února 2014

Termín odevzdání diplomové práce:

27. května 2014

Ve Zlíně dne 7. února 2014

prof. Ing. Vladimír Vašek, CSoc.
děkan



doc. RNDr. Vojtěch Křesálek, CSoc.
ředitel ústavu

ABSTRAKT

Bezpečnostná politika je základný a významný dokument, ktorý rieši komplexné vnímanie bezpečnosti organizácie, alebo spoločnosti. Teoretická časť by mala pojednávať o postavení a štruktúre bezpečnostnej politiky vo vzťahu ku činnosti organizácie. V uvedenej časti práce dochádza ku prezentovaniu teoretických poznatkov k danej problematike. Praktická časť v úvode prezentuje vybraný podnikateľský subjekt a následne analyzuje a vyhodnocuje súčasný stav vzhľadom k plánom a cieľom organizácie. V nasledujúcej časti dochádza ku návrhu opatrení, ktoré naplňujú ciele bezpečnostnej politiky vybranej spoločnosti. Pri návrhu interných smerníc dochádza ku zohľadňovaniu plánov do budúceho vývoja spoločnosti s cieľom vytvoriť vhodné prostredie pre realizáciu plánov. Záver by mal pojednávať o aplikovateľnosti daných smerníc do chodu organizácie, čím by malo dôjsť k zhodnoteniu celkového prínosu bezpečnostnej politiky pre organizáciu.

Kľúčové slová: bezpečnostná politika, analýza, interná smernica, bezpečnostná organizácia

ABSTRACT

Security policy is a fundamental and important document, which addresses the complex perceptions of security organizations or companies. The theoretical section should discuss the status and structure of the security policy in relation to the activities of the organization. In that part of the paper there is the presentation of theoretical knowledge of the problematic. The practical part in the introduction presents selected business entity and then analyzes and evaluates the current situation with regard to the plans and purposes of the organization. In the following occurs to draft measures meeting the goals of the security policy of the selected company. During internal guidelines nomination to the plans, it effectively takes account of the future development of society in order to create a suitable environment for the implementation of plans. Finally, the conclusion discusses the applicability of the guidelines to the organizational processes, which should lead to the assessment of the overall contribution of security policy for the organization.

Keywords: Security policy, Analysis, Internal guidelines, Security organization

PodĎakovanie

Chcela by som poĎakovať mojim rodičom, za podporu, ktorú mi poskytovali počas piatich rokov štúdia a za všetko, čo ma v živote naučili. Chcem poĎakovať môjmu manželovi, ktorý robil všetko pre to, aby mi vytvoril najlepšie podmienky na štúdium a stál pri mne každý deň môjho záverečného ročníka. Moje veľké Ďakujem patrí aj pánovi Ing. Martinovi Hromadovi Ph.D., ktorý mi veľmi pomohol pri písaní diplomovej práce a umožnil mi písanie diplomovej práce pod jeho vedením. Moje Ďakujem patrí všetkým osobám, ktoré mi aj keď nie tak významne, ale určite pomohli pri štúdiu a písaní diplomovej práce.

Prohlašuji, že

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

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD	10
I TEORETICKÁ ČASŤ	12
1 OCHRANA OSÔB A MAJETKU V ŠIRŠOM PRÁVNOM KONTEXTE	13
1.1 PRÁVNÝ RÁMEC SPOJENÝ S BEZPEČNOSTNOU POLITIKOU	13
1.1.1 Listina základných práv a slobôd	13
1.1.2 Občiansky zákonník	13
1.1.3 Obchodný zákonník	14
1.1.4 Trestný zákonník.....	14
1.1.5 Právny rámec ochrany informačných technológií	14
1.1.6 Právny rámec spojený s bezpečnosťou a ochranou zdravia pri práci.....	15
1.1.7 Právny rámec spojený s požiarnou ochranou	16
2 BEZPEČNOSTNÁ POLITIKA	18
2.1 VŠEOBECNÉ BEZPEČNOSTNÉ OPATRENIA	20
2.2 BEZPEČNOSTNÁ ANALÝZA	22
2.2.1 Analýza rizík	23
2.2.2 Bezpečnostná prognóza	24
2.3 STRATEGICKÉ CIELE ORGANIZÁCIE.....	25
2.4 METÓDY ANALÝZ RIZÍK.....	26
2.4.1 Analýza SWOT	28
2.4.2 Úvodná analýza nebezpečenstva.....	29
2.4.3 Štúdiá nebezpečnosti a prevádzkyschopnosti.....	30
2.4.4 Analýza vplyvov porúch a ich následkov	31
2.4.5 Analýza stromom porúch	32
2.4.6 Analýza stromom nebezpečenstva	33
2.4.7 Analýza príčin následkov	33
2.4.8 Analýza spoľahlivosti človeka	34
2.4.9 Paretova analýza	35
2.4.10 Krízová matica.....	35
2.5 BEZPEČNOSTNÉ OPATRENIE PRE MINIMALIZOVANIE RIZIKA V ORGANIZÁCIÍ.....	37
2.5.1 Definovanie fyzickej bezpečnosti organizácie.....	38
2.5.2 Režimové opatrenia.....	38
2.5.3 Definovanie bezpečnostnej dokumentácie	39
2.5.4 Školiace procesy	39
2.5.5 Nastavenie riadenia	40
II PRAKTICKÁ ČASŤ.....	41
3 INFORMÁCIE O SPOLOČNOSTI	42
3.1 CHARAKTERISTICKÁ ŠTRUKTÚRA PODNIKU	43
3.1.1 Obchodné oddelenie podniku	44
3.1.2 Technické oddelenie podniku	44
3.1.3 Oddelenie bezpečnostného manažmentu	47
3.1.4 Oddelenie bezpečnosti informačných technológií.....	47

3.1.5	Ekonomické oddelenie organizácie.....	48
3.1.6	Právnické oddelenie organizácie.....	49
3.1.7	Personálne oddelenie organizácie.....	49
3.2	LOKALIZÁCIA ORGANIZÁCIE.....	50
3.3	STAVEBNÉ DISPOZÍCIE SPOLOČNOSTI.....	51
3.4	PERSONÁLNE ZAISTENIE JEDNOTLIVÝCH FUNKCIÍ.....	52
3.5	CIELE A FUNKCIE PODNIKU.....	58
3.5.1	Potreby potenciálneho zákazníka.....	59
3.5.2	Definovanie procesu získania zákazky.....	60
3.5.3	Definovanie procesu tvorby projektu.....	61
4	ANALÝZA SÚČASNÉHO STAVU.....	63
4.1	BEZPEČNOSTNÉ POSÚDENIE.....	63
4.1.1	Analýza pomocou SWOT analýzy.....	65
4.1.1.1	Všeobecná aplikácia SWOT analýzy.....	65
4.1.2	Analýza pomocou úvodnej analýzy nebezpečenstva.....	67
4.1.3	Analýza vplyvom porúch a následkov v procese organizácie.....	70
4.1.4	Analýza príčin a následkov.....	74
4.1.5	Analýza kompetencií zamestnancov.....	76
4.1.5.1	Obchodné oddelenie.....	76
4.1.5.2	Oddelenie bezpečnostného manažmentu.....	78
4.1.5.3	Technické oddelenie.....	79
4.1.5.4	Oddelenie informačných technológií.....	80
4.1.5.5	Personálne oddelenie.....	82
4.2	BEZPEČNOSTNÁ PROGNOZA.....	83
4.3	DEFINOVANIE ZÁVEROV.....	85
5	NÁVRH BEZPEČNOSTNEJ POLITIKY PODNIKU.....	86
5.1	DEFINOVANIE STRATÉGIE.....	86
5.2	DEFINOVANIE SMERNÍC PRE ZAVEDENIE FYZICKEJ BEZPEČNOSTI OBJEKTU.....	87
5.2.1	Mechanické zábranné systémy.....	88
5.2.2	Poplachový zabezpečovací a tiesňový systém.....	90
5.2.3	Kamerový systém.....	92
5.2.4	Kontrolne dokumenty pre správnu funkčnosť systému.....	93
5.3	DEFINOVANIE SMERNICE PRE PRÍSTUPOVÝ SYSTÉM.....	96
5.4	DEFINOVANIE SMERNICE PRE ČLENENIE JEDNOTLIVÝCH PRACOVÍSK.....	99
5.4.1	Definovanie smernice pre monitorovacie pracovisko.....	99
5.4.2	Definovanie smernice pre riadiace pracovisko.....	103
5.4.3	Definovanie smernice pre vedúce riadiace pracovisko Olomouc.....	106
5.5	DEFINOVANIE SMERNICE PRE URČENIE POŽIADAVIEK NA ZAMESTNANCOV.....	110
5.5.1	Smernica pre technické pracovné pozície.....	111
5.5.2	Smernica pre obchodné pracovné pozície.....	112
5.6	DEFINOVANIE SMERNICE PRE OCHRANU ŽIVOTA A ZDRAVIA OSÔB.....	114
5.6.1	Osobné ochranné a hygienické pomôcky v organizácií.....	119

5.6.2	Požiarna ochrana v organizácií	120
5.7	DEFINOVANIE DOKUMENTÁCIE PRE PLÁNOVANIE	122
5.7.1	Všeobecné požiadavky na systém manažérstva kvality	122
5.7.2	Požiadavky na dokumentáciu systému manažérstva kvality	123
5.7.3	Požiadavky na systém manažérstva kvality z hľadiska zodpovednosti manažmentu	124
5.7.4	Požiadavky na systém preskúmania manažmentom	126
5.7.5	Požiadavky na ľudské zdroje	127
5.7.6	Požiadavky na systém realizácie produktu	127
5.7.7	Požiadavky na návrh a vývoj	128
5.7.8	Požiadavky na systém nákupu	129
5.7.9	Požiadavky na výrobu a poskytovanie služieb	129
5.8	DEFINOVANIE SMERNÍC PRE MERANIE, ANALÝZY A ZLEPŠOVANIE	130
6	APLIKÁCIA A HODNOTENIE NAVRHOVANÝCH POSTUPOV A CIELOV BEZPEČNOSTNEJ POLITIKY	132
6.1	DEFINOVANIE PROCESU HODNOTENIA APLIKOVANÝCH POSTUPOV	132
	ZÁVER	135
	ZÁVER V ANGLIČTINE	137
	ZOZNAM POUŽITÉJ LITERATURY	139
	ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK	141
	ZOZNAM OBRÁZKOV	142
	ZOZNAM TABULIEK	144
	ZOZNAM PRÍLOH	146

ÚVOD

V dnešnej dobe, v ktorej dochádza ku prudkej zmene aspektov pôsobiacich na určitý objekt, hlavne z hľadiska možnosti vzniku hrozby, zisťujeme, že funkcia bezpečnostných riešení je významný aspekt v každej sfére života, a to už či v súkromnom, alebo podnikateľskom prostredí. Každý z nás denne pociťuje hrozbu vzniku nebezpečnej udalosti. Uvedená skutočnosť je spôsobená veľkým počtom faktorov, ktoré na seba vzájomne pôsobia, a tým dochádza ku vzájomnému ovplyvňovaniu. Tak ako rastie hodnota informácií, ktoré potrebujeme chrániť, rastie aj veľkosť hmotného majetku, ale do popredia vystupuje aj hodnota duševného vlastníctva a know how. No nie je to len o tom, že hodnota uvedených produktov a služieb rastie, ale aj o skutočnosti, že povedomie a vedomosti potenciálnych páchatel'ov veľmi rýchlo napredujú, a môže dochádzať ku situáciám, kedy ochrana určitého produktu je neúčelná, a to z dôvodu, že páchatel' je nadmieru vzdelaný a informovaný o možnosti prekonania zábrany bez jej porušenia, alebo vyvolania poplachu. Keď chceme definovať potenciálneho páchatel'a, musíme si uvedomiť, že sa nejedná len o ľudí na okraji spoločnosti, ale že veľmi často dochádza k útoku na spoločnosť veľmi vysoko postavenými osobami, dokonca je možné povedať osobami vo vedúcom postavení.

Do popredia vystupuje konkurenčný boj a boj o zákazníka, kedy každá informácia o chode konkurenčného podniku je významnou informáciou, alebo znemožnenie funkčnosti určitého komponentu konkurenčnej spoločnosti aspoň na krátky časový interval, spôsobí nárast počtu klientov o významnú hodnotu. Nie vždy samotné poškodenie môže vyvolať daný efekt, ale len spochybnenie o správnom fungovaní organizácie môže spôsobiť presun veľkého počtu klientov na opačnú stranu konkurenčného boja, a tým získanie prevahy. Dôvodov, prečo by mala organizácia zavádzať bezpečnostné opatrenia je veľa, no hlavný je zaistiť bezpečnú prevádzku. V prípade výrobných organizácií je priamo nevyhnutné definovať daný dokument. V prípade poskytovania služieb je uvedený dokument prinajmenšom vhodným dokumentom. Ale ak hovoríme o spoločnosti, ktorá plánuje rozvoj svojej činnosti a samotná sa zaoberá bezpečnosťou, je veľmi potrebné, aby uvedený dokument bezpečnostnej politiky mala spracovaný na kvalitnej úrovni, tak aby mohlo dochádzať ku strategickým zmenám vzhľadom na plány rozvoja spoločnosti do budúcnosti. Je možné povedať, že bezpečnostná politika môže pomôcť organizácii pri vytváraní prostredia, v ktorom je uchytenie aplikovateľnosti novej stratégie pravdepodobnejšie, ako bez zavedenia bezpečnostnej politiky. Každá organizácia má časti bezpečnostnej politiky

v rámci interného, alebo dokonca aj externého riadenia, no nie vždy si uvedomuje potrebu a dôležitosť daných informácií a potrebu dodržiavania jednotlivých požiadaviek. Ak vytvoríme jeden dokument, ktorý bude zoskupovať dané pravidlá je pravdepodobnejšie ich pochopenie v naviazanosti na iné bezpečnostné pravidlá a hlavne dochádza k ľahšiemu pochopeniu aplikovateľnosti do celkového procesu chodu organizácie.

Ak predvídame, že daná hrozba existuje, máme náskok, pretože máme čas na odstránenie vyvolávajúcich aspektov. Ak si ale myslíme, že správne je zabezpečiť sa iba proti hrozbe, ktorá hrozí dnes, naša existencia v budúcnosti bude ohrozená. To, že hrozbu organizácia nevidí, neznamená, že hrozba neexistuje, môže to ale znamenať, že jej prepuknutie spôsobí katastrofálne následky.

I. TEORETICKÁ ČASŤ

1 OCHRANA OSÔB A MAJETKU V ŠIRŠOM PRÁVNOM KONTEXTE

Aplikovanie bezpečnostnej politiky by malo umožniť stanovenie procesov, ktoré definujú rozsah školení, ale aj aplikácií jednotlivých technológií, a to za cieľom znížiť pravdepodobnosť výskytu hrozby. Z hľadiska právneho kontextu, sa jedná o súhrn definovaných smerníc, podľa ktorých, by sa mali zamestnanci, ale aj osoby nachádzajúce vo vzťahu k organizácií správať, a nadobudnutím určitého právneho stavu, sa zaviazat' k napĺňovaniu uvedených pravidiel. Interné smernice sú už výsledkom stanovenia bezpečnostnej politiky, ktorá je určená na základe právnych predpisov Českej republiky, charakterom činnosti danej organizácie, ale aj technickými normami a inými špecifikáciami, ktoré sa daná organizácia zaviazala plniť pri nadobudnutí vzťahu s inou treťou stranou.

1.1 Právny rámec spojený s bezpečnostnou politikou

V súčasnej dobe dochádza ku riešeniu bezpečnostnej politiky z komplexného pohľadu, čo by malo viesť k poznaniu jednotlivých právnych úprav danej oblasti, ktorej sa venuje podnikateľský subjekt. V prípade, že sa jedná o podnik z viacerými odvetvami podnikateľských aktivít, je nutné na daný subjekt pozerat' z pohľadu systému tvoreného subsystémami, ktoré musia spĺňovat' uvedené právne predpisy, ale zároveň by mali spĺňovat' predpisy týkajúce sa ich pôsobenia z hľadiska vzájomných väzieb.

1.1.1 Listina základných práv a slobôd

K vyhláseniu listiny základných práv a slobôd došlo ustanovením zákona č. 2/1993 Sb., jedná sa o vyššiu právnu normu, a teda je nutné, aby dochádzalo k jej rešpektovaniu z hľadiska bezpečnostnej politiky podniku. Je nutné bezpečnostnú politiku stanoviť tak, aby napĺňovaním jednotlivých plánov bezpečnostnej politiky nedochádzalo k neoprávnenému zásahu do práv a slobôd zamestnancov, ale aj zákazníkov a iných osôb, ktoré sú spojené s podnikom a dotýka sa ich bezpečnostná politika firmy.

1.1.2 Občiansky zákonník

Občiansky zákonník reprezentuje v účinnosti od 1.1.2014 nový zákon č. 89/2012 Sb., ktorý je v súčasnosti považovaný za doposiaľ najväčšiu premenu pôvodného zákona č. 513/1991

Sb., ktorý bol priebežne upravovaný. Z pohľadu bezpečnostnej politiky sa jedná o deklarovanie ochrany práv právnických a fyzických osôb, ale aj o získanie práva k nehnuteľnosti, predkupného práva a susedských vzťahov. (Zákon č. 89/2012 Sb. o Občianskom práve)

1.1.3 Obchodný zákonník

Zákon č. 513/1991 Sb. definuje obchodný zákonník, ktorý upravuje vzťahy súvisiace s podnikaním, postavenie podnikateľov, obchodné vzťahy a príslušné predpisy Európskych spoločností. Súčasne je nutné poznamenať, že od 1.1.2014 dochádza ku platnosti Zákona o obchodných korporáciách zákonu č. 90/2012 Sb., ktorý v určitej časti nahradzuje obchodný zákon. Ak definujeme bezpečnostnú politiku podniku dochádza ku vymedzeniu podnikateľskej činnosti a obchodných vzťahov.

1.1.4 Trestný zákonník

Trestný zákonník definuje zákon č. 40/2009 Sb., ktorý pojednáva o ochrane osôb a majetku, upravuje trestné právo hmotné, definuje jednotlivé akty spojené s trestnou činnosťou a trestné sankcie. V druhej časti dochádza k definovaniu podstaty trestných činnou, ktoré sú spojené s ľudskou dôstojnosťou, rodinnou a životným prostredím. Uvedený zákonník môžeme definovať, ako jeden s primárnych pilierov bezpečnosti a charakteristiky podvodu, krádeže a sankcií za jednotlivé trestné činy. (Zákon č. 40/2009 o trestnom práve)

1.1.5 Právny rámec ochrany informačných technológií

V prípade, že chceme stanoviť bezpečnostnú politiku organizácia je nevyhnutné analyzovať bezpečnosť informačného systému, a to z dôvodu, že vo vývoji súčasných technológií narastá riziko straty, alebo scudzenia práve prostredníctvom informačných technológií. V prípade spoločnosti je nutné rešpektovať zákon č. 101/2000 Sb. o ochrane osobných údajov, a to hlavne z dôvodu, že jeho účelom je ochrana pred neoprávneným zásahom do súkromia osoby. Pri uvedenej problematike je nutné taktiež dohliadať na dodržanie zákona č. 227/2000 Sb., ktorý definuje poskytovanie certifikačných služieb a používanie elektronického podpisu. O utajovaných informáciách pojednáva zákon č. 412/2005 Sb. a je nevyhnutné jeho znenie rešpektovať pri definovaní bezpečnostnej politiky organizácie.

Informačný systém integrovaný do firemného procesu, uľahčuje prácu, ale zároveň predstavuje obrovskú hrozbu pre spoločnosť, a to v prípade, že dochádza ku spracovávaniu hodnotných dát pre firmu, alebo aj spracovávanie dát ohľadne zamestnancov a klientov, ktoré je potrebné chrániť, aby nedochádzalo k ich zneužitiu a mohlo by dôjsť k poškodeniu firmy, ale aj inej firmy s ktorou uvedená spoločnosť prichádza do styku, alebo je medzi uvedenými firmami vzájomný obchodný vzťah.

Tab. 1. Definovanie základných právnych predpisov o bezpečnostnej politike [18]

Zákon č. 121/2000 Sb.	Zákon o autorskom práve a o právach súvisiacich s autorským právom
Zákon č. 127/2005 Sb.	Zákon o elektronickej komunikácii
Zákon č. 206/2005 Sb.	Zákon o ochrane služieb v oblasti rozhlasového a televízneho vysielania
Zákon č. 56/2006 Sb.	Zákon o prevencii závažných havárii
Zákon č. 480/2004 Sb.	Zákon o službách informačnej bezpečnosti
Vyhláška č.366/2000 Sb.	Vyhláška k zákonu o elektronickej podpise
Vyhláška č.523/2005 Sb.	Vyhláška o bezpečnosti informačných a komunikačných systémov

1.1.6 Právny rámec spojený s bezpečnosťou a ochranou zdravia pri práci

Dokument pojednávajúci o bezpečnosti a ochrane zdravia pri práci je jedným z významných dokumentov bezpečnostnej politiky podniku. Právne predpisy definujúce podmienky BOZP:

- Zákon č. 262/2006 Sb. upravujúci pracovne právne vzťahy,
- Zákon č. 309/2005 Sb. o zaistení ďalších podmienok pre BOZP,
- Zákon č. 174/1968 Sb. o štátnom odbornom dozore BOZP,
- Zákon č. 251/2005 Sb. o inšpekcií práce,
- Nariadenie vlády č. 93/2012 Sb. stanovujúce podmienky ochrany zdravia pri práci,
- Smernica č. 89/391 EHS o zavedení opatrení pre zlepšenie bezpečnosti a ochrany zdravia pri práci,
- Smernica č. 89/654 o minimálnych požiadavkách na bezpečnosť a ochranu zdravia na pracovisku. [18]

1.1.7 Právny rámec spojený s požiarou ochranou

Jedným s primárnych legislatívnych dokumentom v oblasti požiarnej ochrany je zákon o požiarnej ochrane č. 133/1985 Sb., kde dochádza k uvedeniu základných povinností pre fyzické a právnické osoby v oblasti požiarnej ochrany. Uvedený zákon dopĺňa vyhláška o požiarnej prevencii č. 246/2001 Sb. Medzi ďalšie zákony spojené s požiarou ochranou patria nasledujúce:

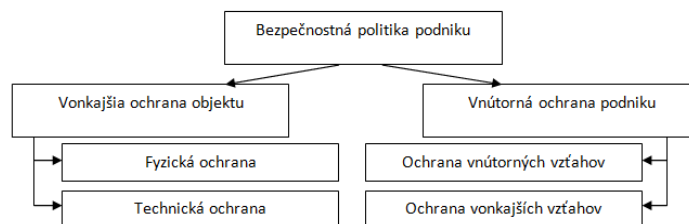
- Zákon č. 238/ 2000 Sb. o hasičskom záchrannom zbore,
- Zákon č. 183/ 2006 Sb. o územnom plánovaní a stavebnom poriadku,
- Zákon č. 133/ 1985 Sb. o požiarnej ochrane v znení neskorších predpisov,
- Zákon č. 11/ 2000 Sb. stanovuje vzhľad a umiestnenie bezpečnostných značiek a zavedenie signalizácie,
- Zákon č. 239/ 2000 Sb. o integrovanom záchrannom systéme a zmene niektorých zákonov,
- Nariadenie vlády č. 91/ 2010 Sb. o podmienkach požiarnej bezpečnosti pri prevádzke komínov a spotrebičov palív,
- Vyhláška č. 202/199 Sb., ktorou sú stanovené technické podmienky požiarnej dverí,
- Vyhláška č. 23/ 2008 Sb. o technických podmienkach požiarnej ochrany stavby,
- Vyhláška 268/ 2000 Sb. o technických požiadavkách na stavby,
- Vyhláška č. 24/ 2001 Sb. o stanovení podmienok požiarnej bezpečnosti a výkonu štátneho požiarneho dozoru,
- Vyhláška č. 499/ 2006 Sb. o dokumentácii stavieb,
- Vyhláška č. 73/ 2010 Sb. o stanovení vyhradených technických zariadení,
- Vyhláška Národného bezpečnostného úradu č. 258/1998 Sb. o objektivej bezpečnosti.

Uvedený právny rámec je orientačný a na primárnej úrovni. Pre optimálne riešenie by mal byť doplnený o technické normy a špecifikácie iného rozsahu, ktoré sa organizácia zaviazala plniť, alebo ich plnenie je nevyhnutné z dôvodu zákonnej požiadavky. V uvedenej kapitole došlo k všeobecnému popisu Listiny základných práv a slobôd, Občianskeho zákonníka, Obchodného zákonníka, Trestného zákonníka a právnych predpisov spojených s ochranou informačných technológií, ako aj s bezpečnosťou a ochranou zdravia pri práci

a v neposlednom rade aj s požiarou ochranou. Uvedený právny rámec je základný pre uvedenie si požiadaviek zo strany organizácia na jednotlivé právne odvetvia.

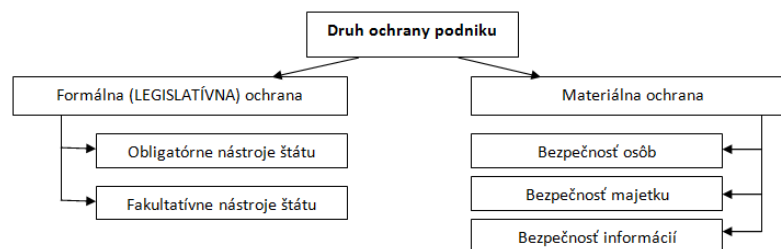
2 BEZPEČNOSTNÁ POLITIKA

Uvedená časť práce pojednáva o postavení bezpečnostnej politiky v súčasnom sektore podnikania, a to vedie k vysloveniu primárnych princípov, ktoré definujú, akým spôsobom by mal byť chránený podnik. Predmet záujmu bezpečnosti môžeme definovať, ako ochranu života, teda osôb, hmotného majetku, a majetku nehmotného (poprípade know how). Uvedená časť práce sa zameriava na metódy analýzy jednotlivých funkcií podniku, pričom dochádza ku definovaniu zodpovedností. Bezpečnostná politika je vo všeobecnosti chápaná, ako systém pravidiel, ktoré spolu vytvárajú také prostredie, v ktorom je miera vzniku rizika minimalizovaná na najnižšiu možnú úroveň, a teda dochádza k vytvoreniu optimálneho prostredia ku naplneniu strategického plánu podniku. Bezpečnostnú politiku podniku je nutné chápať, ako zložitý systém tvorený subsystémami, ktoré majú definované subciele a spoločne naplňajú jeden cieľ.



Obr. 1. Rozdelenie systému bezpečnostnej politiky podniku na subsystém [2]

V prípade, že sa na analýzu zameriame pomocou rozboru systémy ochrany podniku, dôjdeme k záveru, že je možné rozdeliť ochranu podniku na dva primárne druhy.

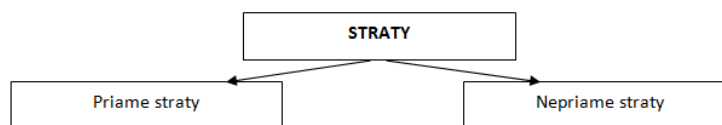


Obr. 2. Definovanie druhov ochrany podniku [12]

V prípade, že chceme definovať legislatívne nástroje štátu, alebo podniku, určíme ich účel vzhľadom ku bezpečnosti daného systému. Legislatívne nástroje štátu sú využívané na stanovenie jednotných bezpečnostných štandardov, a to v rámci celej spoločnosti. Formálna ochrana zahŕňa konkrétne a presne vymedzený právny rámec, ktorý je stanovený,

presadzovaný a kontrolovaný štátom a musí dochádzať k jeho bezpodmienečnému plneniu. Je to obligatórny nástroj štátu, teda jeho plnenie je všeobecne dané a nutné. Ďalší druh ochrany je zaisťovaný pomocou legislatívy stanovenej štátom, ktorá slúži na presadzovanie štátnych záujmov. Medzi jej funkcie je možné zahrnúť reguláciu pracovne právnych, alebo obchodných vzťahov. Dochádza tiež k stanoveniu určitého rozmedzia v ktorom sa podniky môžu pohybovať. Uvedené nástroje sú zaradované medzi fakultatívne nástroje riadenia, čo znamená, že v prípade ich použitia dochádza k vzájomnej dohode medzi zmluvnými stranami, a teda napríklad medzi zamestnancom a zamestnávateľom. Posledný druh ochrany je charakterizovaný, ako legislatívne nástroje podniku, ktoré konkretizujú zásady riadenia podniku. Uvedený nástroj je používaný, ako nástroj na aplikovanie všeobecných podmienok stanovených orgánmi štátu do konkrétnych podmienok podniku. [12]

V prípade, že hrozí riziko straty, je nutné si definovať povahu straty, ktorá hrozí.



Obr. 3. Definovanie povahy straty [12]

Priame straty môžeme definovať, ako straty, ktoré je možné priamo vyčíslieť. Medzi uvedené straty patrí krádež, lúpež, zverejnenie obchodného tajomstva, alebo stratégií. Dochádza ku škode nielen materiálnej, ale aj ku škode duševnej povahy. Vo všeobecnosti je známi fakt, že jedna priama strata spôsobí približne šesť druhov nepriamej straty, ako príklad uvedieme požiar výrobného haly. Priama strata je strata výrobného haly. Nepriama strata je dlhodobé prerušenie výroby, zničenie strojov a výrobného materiálu, nutné náklady na nové stroje, nutná celozávodná dovolenka, zníženie produktivity podniku a iné. Z uvedeného príkladu je možné formulovať záver, že v prípade analýzy je nutné aj riziko charakterizované nízkou hodnotou zanalyzovať vzhľadom na jeho možné negatívne pôsobenie prejavujúce sa v nepriamych stratách, a to až na pokročilej úrovni jeho pôsobenia. V prípade, že bude dochádzať k analýze do podrobného možného stavu, dôjde aj k odhaleniu latentného rizika a možných vysokých nepriamych strát, a tým dôjde aj k znovu prehodnoteniu istej udalosti a tým k presnejšiemu hodnoteniu novej hrozby.

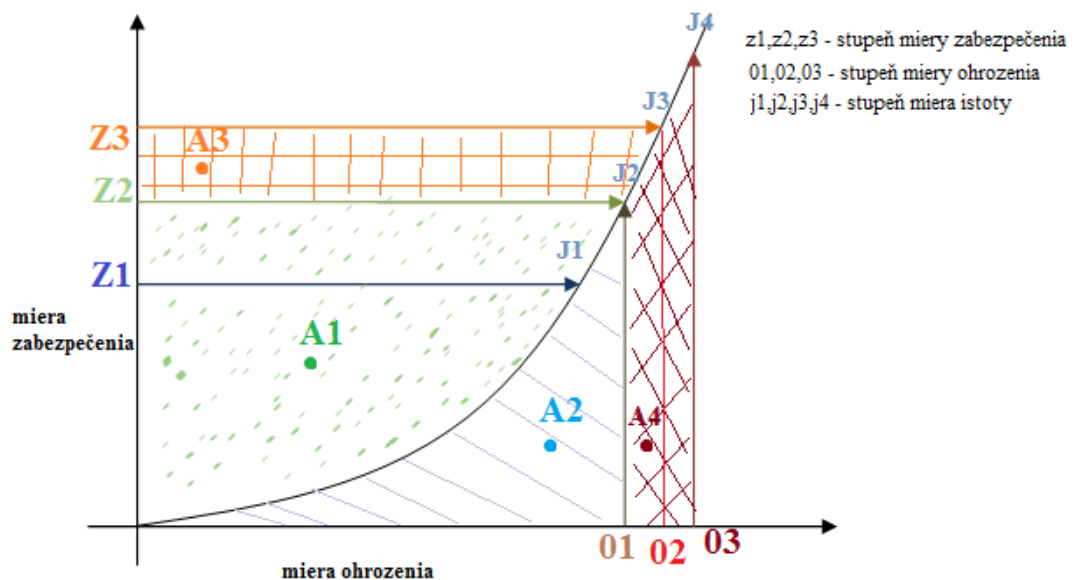
2.1 Všeobecné bezpečnostné opatrenia

Všeobecné bezpečnostné opatrenia, by mali vytvárať bezpečnostnú politiku podniku, a to za pomoci ochrany života a zdravia, ktorá je spojená so samostatnou ochranou obyvateľstva. Malo by dochádzať k chráneniu všetkého, čo je spojené s vlastníckymi vzťahmi, a to k hmotným, ale aj nehmotným veciam, teda materiálna existencia. Malo by dochádzať k ochrane všetkého, čo je spojené s presadzovaním a ochranou jednotlivých osôb, teda ku ochrane spoločenskej existencie. Medzi uvedenými hlavnými všeobecným opatreniami je možné definovať vzájomné ovplyvnenie, ktoré môže vyvolať udalosť, že narušenie jedného záujmu môže vyvolať narušenie iného záujmu. Z uvedeného dôvodu, je nutné si uvedomiť, že tak ako následok môže mať veľký počet príčin, tak aj príčina môže vyvolať veľký počet následkov. Typicky viditeľným znakom bezpečnostných opatrení je to, že každé opatrenie po určitej dobe stráca na miere svojej účinnosti. Ak v minulosti plnil svoj účel zabezpečenia vodný výkop, ktorý bol situovaný v okolí hradu, tak po čase svoj účel stráca. Uvedený proces je prirodzený a súvisí s rozvojom technológií, ale aj s prekonávaním psychologických bariér. V uvedenom prípade nie je vylúčené, že k prekonaniu určitej prekážky môže dôjsť použitím vyspelejšej zbrane, ale aj zmenou taktiky, alebo prístupu. [1]

Z minulosti je možné definovať všeobecné bezpečnostné aspekty na definovanie primárnych skutočností, ktoré sú aplikovateľné aj v dnešnej dobe a sú všeobecne platné:

- Cieľ zabezpečenia – definovanie žiadaného stavu,
- Objekt zabezpečenia – život a zdravie osôb, inštitúcia, organizácia,
- Spôsoby a prostriedky zabezpečenia,
- Materiálové a finančné náklady na prevedenie zabezpečenia,
- Termíny pre realizáciu,
- Osoby zodpovedné za prevedenie zabezpečenia. [1]

Medzi primárne aspekty taktiež patrí určenie minimálnych podmienok, ktoré musia byť splnené pre dosiahnutie požadovanej úrovne zabezpečenia, aby došlo k zabezpečeniu mieri bezpečnosti, a teda istoty. Úroveň, účinnosť, použité prostriedky a náklady na zabezpečenie sú priamou reflexiou mierou nebezpečenstva alebo ohrozenia. Na nasledujúcom obrázku je zobrazená závislosť medzi mierou zabezpečenia a mierou ohrozenia.



- A1** - miara zabezpečenia, ako systém prostriedkov ku zníženiu eliminácii miery ohrozenia
A2 - miara ohrozenia, ako súhrn použitých možných útočných prostriedkov a hrozieb vedúcich k ohrozeniu a prekonaniu zabezpečeniu
A3 - navýšenie miery zabezpečenia nutné k vyrovnaniu nárastu miery ohrozenia označenej 02
A4 - nárast miery ohrozenia, ktorý by mal byť vyrovnaný nárastom miery zabezpečenia

Obr. 4. Vzťah miery zabezpečenia na miere ohrozenia [1]

Uvedený obrázok definuje vzťahy medzi mierou ohrozenia a mierou zabezpečenia. Z uvedeného obrázku vyplýva, že ak narastie miara ohrozenia, tak je nutné aby narástla aj miara zabezpečenia, ak naším cieľom je zabezpečiť optimálnu úroveň bezpečnosti. V inom prípade, ak nedôjde ku zvýšeniu miery zabezpečenia, tak sa účinnosť zabezpečenia zníži, a teda nebude naplnený cieľ zabezpečenia. Dôjde ku strate istoty, alebo k zníženiu pod akceptovateľnú úroveň. Prostriedky ohrozenia sú v stálom vývoji, a teda dôjde ku nutnosti realizovať analýzy v časových intervaloch a reagovať tým na zmeny vo vývoji. Žiaduci stav je možné definovať, ako rovnováhu medzi mierou ohrozenia a mierou zabezpečenia. Ak dochádza k situáciám, kedy miara zabezpečenia nezodpovedá miere ohrozenia, dochádza k poddimenzovaniu celého systému, a teda nedochádza k eliminácii možného nebezpečenstva.

Všeobecné ochranné opatrenia je možné definovať nasledovne:

- Vytváranie celkovej bezpečnostnej politiky podniku, alebo inštitúcie,
- Zaisťovanie fyzickej ochrany objektov, majetku, osôb a informácií,
- Programovo technické opatrenia v automatizovaných informačných systémoch, týkajúcich sa software, hardware, riadneho vedenia potrebnej dokumentácie, protívirusové opatrenia,
- Organizačne- režimové opatrenia, k nim patrí jasné a presné vymedzenie funkcií, kompetencií, režimu v objektoch, hierarchickej úrovne pracovníkov,
- Personálne opatrenia pri výbere a kontrole ľudských zdrojov.

Z hľadiska ochrany jednotlivých objektov je možné rozlišovať nasledujúce druhy opatrenia:

- Organizačné – organizačný poriadok, pracovný poriadok, technologické postupy,
- Administratívne – predpisy, pokyny, smernice a iné,
- Režimové – pokyny pre činnosť v krízových opatreniach, rozdelenie režimov,
- Právne – preventívne a represívne,
- Fyzické – predpisy stavebné, elektrotechnické, vzduchotechnické,
- Technické – pre hardware a software,
- Personálne – pre výber a výchovu personálu.

Ochranu podniku môžeme definovať ako komplex systémových, materiálnych, organizačných (administratívnych a režimových), technických, personálnych a sociálne psychologických opatrení s cieľom minimalizovať možné straty vlastníctva. [12]

2.2 Bezpečnostná analýza

Bezpečnostná analýza je metóda používaná pre proces syntézy získaných poznatkov a vypracovanie bezpečnostného projektu, ktorého hlavnou úlohou je stanoviť konkrétne body a opatrenia, pri ich naplnení dôjde ku dosiahnutiu vytýčeného cieľa bezpečnostnej politiky. Bezpečnosť je nutné pochopiť, ako celok, teda systém, ktorý je vytvorený pre dosiahnutie určitého, dopredu stanoveného cieľa. Prvky tohto systému sú spojené logickými väzbami, ktoré majú svoje zákonitosti. Uvedený systém je funkčnosti schopný, ak je

schopný reagovať v čase na určité zmeny, a teda je schopný sa operatívne prispôbiť, a to bez obmedzenie jeho funkcie. Medzi uvedené zmeny, na ktoré musí systém reagovať nepatria len zmeny vychádzajúce z minulosti a prítomnosti, ale aj predvídané zmeny v budúcnosti. Budúci vývoj je formulovaný vo forme bezpečnostnej prognózy. Nie je možné posudzovať budúcnosť len na základe minulosti a prítomnosti. Pri posudzovaní pravdepodobnosti budúcich situácií je nutné zohľadňovať aj menej pravdepodobnostné stavy. Každá analýza a posudzovanie musí zachovať systémový prístup.

Stanovenie bezpečnostnej analýzy a definovanie prístupu ku jej spracovaniu:

1. Formulácia problému a cieľu bezpečnostnej analýzy.
2. Stanovenie zásad pre prístup k riešeniu problému – definovanie vzťahu s právnymi zákonmi, technickými normami a inými záväznými dokumentmi.
3. Zber potrebných informácií, ktoré sú získavané na ďalšiu analýzu a syntézu
4. Analýza a syntéza získaných poznatkov a informácií.
5. Analýza kritérií ochrany bezpečnosti firmy, definovanie hroziaceho rizika a definovanie súčasného stavu.
6. Interpretácia spracovania informácií s ohľadom na vypracovanie výstupu, ktorý slúži, ako vstup pre vypracovanie bezpečnostnej prognózy.

2.2.1 Analýza rizík

Pre bezpečnostné analýzy sú veľmi častou využívané analýzy z iného odvetvia, ktoré sú následne modifikované na obor bezpečnosti danej organizácie, alebo podniku. Hlavnou časťou každej bezpečnostnej analýzy je analýza rizík, ktorá plní hlavnú rolu v stave určovania a posudzovania bezpečnosti inštitúcie. Analýza rizík by mala nájsť odpoveď na nasledujúce otázky:

- Aké riziká, alebo hrozby môžu v danom subjekte nastať,
- Aká je pravdepodobnosť vzniku, že definované hrozby nastanú, a teda dôjde k vyvolaniu bezpečnostného konfliktu,
- Aké budú následky, keď uvedené bezpečnostné konflikty nastanú.

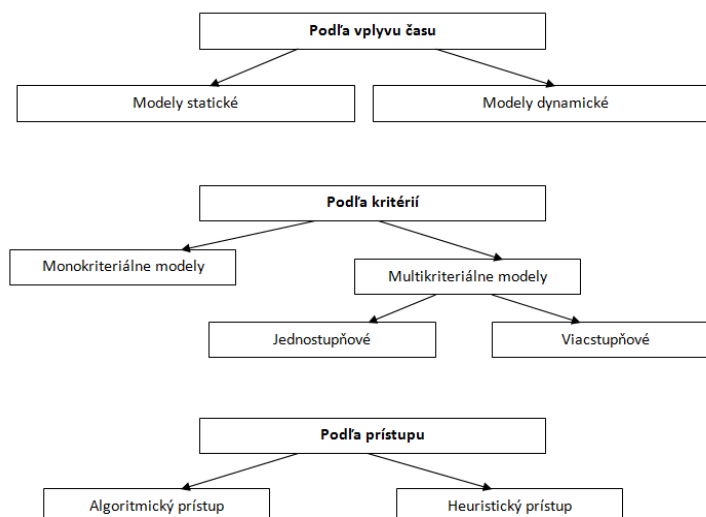
Formulovaním odpovedí na uvedené otázky, nám bude ľahším spôsobom umožnené formulovať, aké opatrenia je nutné stanoviť na dosiahnutie cieľa. [1]

2.2.2 Bezpečnostná prognóza

Bezpečnostnú prognózu môžeme chápať, ako predvídanie určitého kladného, alebo záporného protiprávneho, proti firemného, alebo iného nežiaduceho jednania skupiny, alebo jednotlivca v určitom časovom intervale, ktoré negatívne ovplyvňuje bezpečnosť podniku, alebo firmy.

V prípade prognózovania bezpečnostných stratégií v podniku dochádza ku použitiu kriminalistického prístupu, a to hlavne z dôvodu, že kriminalistika spracovala veľký počet metód, ktoré zabezpečia opatrenia v oblasti spoločenských vzťahov.

V prípade prognózy je využívaný modelový prístup, kedy dochádza k modelovaniu jednotlivých možných prognózovaných stavov a následne je možné realizovať niekoľko variant riešenia, a teda dochádza k uľahčeniu procesu hodnotenia a definovaniu najadekvátnejšieho postupu, a to priamo v procese prognózovanej situácie. Rozhodovací proces v procese modelovania umožňuje alternatívne prístupy k riešeniu problému. V prípade rozdeľovania metód prognózovania dochádza k hodnoteniu podľa viacerých kritérií. Uvedené zobrazenia sú zobrazené na nasledujúcom obrázku.



Obr. 5. Rozdelenie typológie prognózovania [2]

Modely statické reprezentujú systémy, ktoré sa v čase nemenia. Uvedené systémy disponujú s kombinačným jednaním, kde dochádza k reakciám, ktoré sú určené súčasným a trvajúcim

stavom podnetu. Na rozdiel od modelov statických, existujú modely dynamické, ktoré formulujú problém, ktorého sa stav v časovom intervale mení. Monokriteriálne modely reprezentujú modely, ktoré sú hodnotené len z jedného hľadiska. Uvedené modely sú veľmi málo používané v bezpečnostnej politike podniku, a to z dôvodu, že uvedené modely riešia len jedno odvetvie, teda problém je len v jednej dimenzii podniku. Multikriteriálne modely sú založené na riešení problému komplexne s ohľadom na účelné kritéria v ich vzájomných väzbách a vzťahoch, a výsledok je zobrazovaný integrovane.

Prognostické modelovanie a prognostické modely sú charakterizované prístupmi, ktorými sa k určitému problému pristupuje. Algoritmický prístup je definovaný pomocou zachovania poradia krokov tak, aby vždy došlo ku rovnakému riešeniu. V bezpečnostnom prognózovaní sa uvedená metóda využíva čiastočne na riešenie pod problému. Dochádza k presnému určeniu sledu základných operácií a následne je možné uvedené kritéria kvantifikovať a vytvoriť matematický model riešenia. Heuristický prístup v bezpečnostnom prognózovaní je možné definovať, ako metódu určenia postupu pri nových informáciách, alebo stavoch. Primárny základ uvedeného prístupu je, že využíva logický úsudok a odborné skúsenosti.

2.3 Strategické ciele organizácie

V prípade, že definujeme bezpečnostnú politiku podniku je nutné definovať si problém, na ktorý je následne definovaný postup, ktorý reprezentuje alternatívne riešenia problému, ktoré sú znovu zhodnotené, a teda dochádza ku výberu vhodnej alternatívy, ktorá je modelovou aplikáciou uvedená do podniku a následne dochádza k overeniu predpokladaného výsledku a implementácií opravných postupov. Pri komplexnom prístupe, ktorý by mal byť realizovaný, ak chceme definovať bezpečnostnú politiku celej organizácie, je nutné prihliadať na väzby, ale aj iné strategické ciele, a to tak, aby nedochádzalo ku ich vzájomnému negovaniu, alebo zníženiu účinnosti jednotlivých strategických plánov.

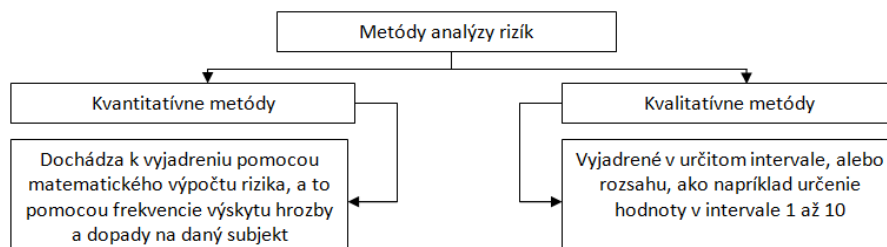
Strategický cieľ je dosahovaný pomocou strategických plánov, ktoré nie sú vždy výlučne o je definované v oblasti bezpečnosti. Každá zmena v časovom intervale, ktorá má dlhodobý charakter a môže ovplyvniť vývoj firemného prostredia, ovplyvňuje aj strategické ciele, a preto je nutné uvedené plány kontrolovať a znovu analyzovať účinnosť plánov. V prípade definovania bezpečnosti podniku, je nutné interné strategické ciele poznať a porozumieť

celkovej vnútornej harmónii podniku, ale hlavne definovať ciele do budúceho vývoja, a to jednotlivých oddelení, ale aj celej firmy.

Veľmi veľký počet relevantných informácií sa nachádza v medzinárodných zmluvách a štandardoch, ale aj v právnych predpisoch. Pri získavaní informácií sú analyzované jednotlivé funkcie v podniku, personálne požiadavky, ale aj vzťahy medzi dodávateľmi a architektonické a stavebné plány.

2.4 Metódy analýz rizík

Metódy analýzy rizika je možné deliť z viacerých pohľadov, podľa ktorých sú dané metódy zoskupované do skupín. Každá analýza vyhodnocuje určité rizikové údaje podľa zvolených kritérií a následne dochádza k vysloveniu záveru na základe ktorého dochádza k uvedomeniu si jednotlivé váhy rizík, ktoré organizácií hrozia. Jednotlivé metódy vznikli prevzatím od jednotlivých organizácií, v ktorých boli vyvinuté na sledovanie a hodnotenie výskytu rizika. V prípade použitia v určitej organizácii nedochádza k aplikácii len jednej metódy, ale ku kombinácii viacerých metód.



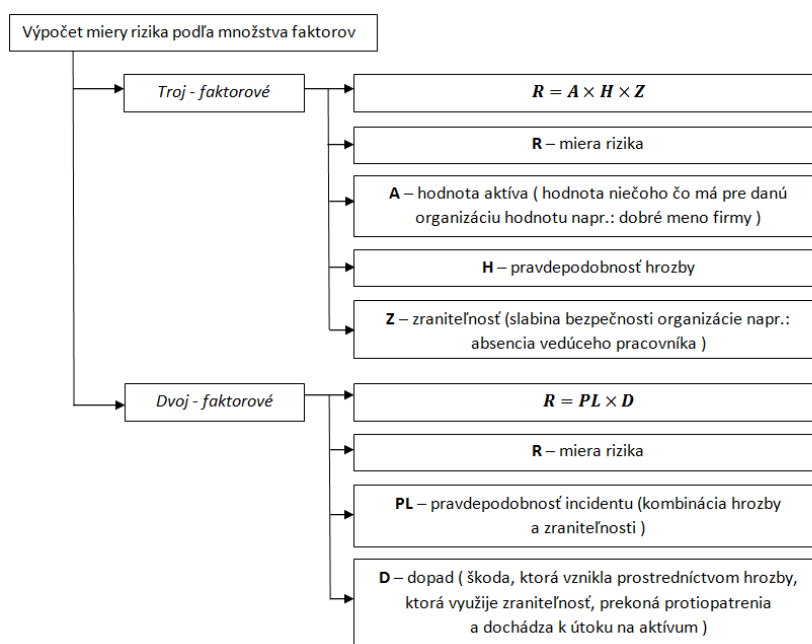
Obr. 6. Kvantitatívne a kvalitatívne metódy analýzy rizík [6]

Kvalitatívne metódy sú považované za rýchlejšie a jednoduchšie, ako metódy kvantitatívne. Dochádza k problému s efektivitou nákladov. Kvantitatívne metódy sú všeobecne považované za exaktné, ale náročnejšie na čas a úsilie. Jednou z hlavných výhod použitia kvantitatívnych metód je možnosť určenia finančného vyjadrenia rizika.

Medzi kvalitatívne metódy patrí metóda účelových interview, tiež nazývaná, ako metóda Delphi. Určená metóda je založená na riadení kontaktu a komunikácie medzi expertmi, ktorí sa zúčastňujú na hodnotení, a teda sú súčasťou hodnotiacej skupiny danej organizácie, alebo určitého problému. K použitiu aplikácie rizikovej analýzy dochádza ku prediskutovaniu súboru otázok na účelových pohovoroch, pričom otázky sú tvorené dvoma časťami. Prvá

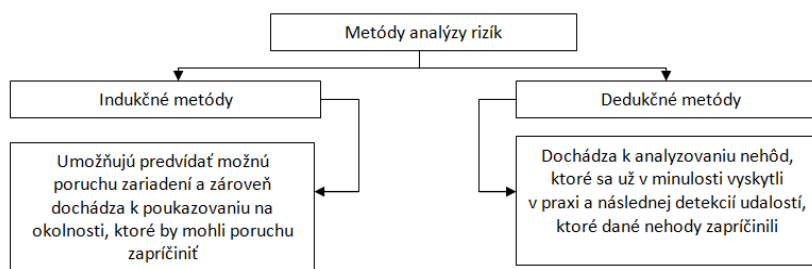
časť otázky je dopredu stanovená a druhá časť je variabilná a dochádza k jej obmeňovaniu v priebehu pohovoru. Uvedená metóda býva aplikovaná v procese iteračne, teda viacúrovňovo.

Kvantitatívne metódy sú vo väčšine prípadov aplikované v oblasti bezpečnosti organizácií a v hodnotení informačných systémov. Jednou z uvedených metód je metóda CRAMM, ktorá skúma model určitého systému. Kvantitatívne metódy analýzy rizika sú založené na matematickom výpočte miery rizika z frekvencie výskytu hrozby a následného dopadu na danú organizáciu.



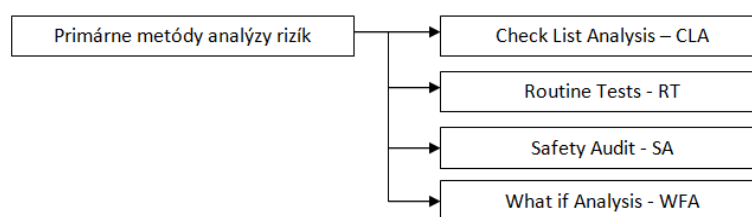
Obr. 7. Výpočet miery rizika podľa kvantitatívnej metódy [4]

Medzi jedno z možných rozdelení patrí rozdelenie metód analýzy rizika na indukčné a dedukčné metódy, ktoré analyzujú nehody a predvídajú možné poruchy.



Obr. 8. Indukčné a dedukčné metódy analýzy rizík [6]

Ak dochádza ku analýze rizika, dochádza k použitiu a aplikovaniu jednotlivých metód do procesu, v ktorom by malo dôjsť ku vyhodnoteniu rizika, a tým k odhaleniu potenciálnej hrozby. Vo všeobecnosti je možné konštatovať, že v rámci podniku, alebo firmy dochádza k veľkému počtu používaných metód, ktoré jednotlivo odhaľujú riziká spojené s konkrétnou činnosťou a veľa krát nastáva situácia, kedy sa nejedná o analýzu, ktorá primárne má určiť rizikový faktor, alebo odhaliť riziko, ale napriek tejto skutočnosti poukazuje na daný problém, a teda plní vedľajšiu úlohu.



Obr. 9. Primárne metódy používané na analýzu rizík [16]

Metóda CLA, tiež prekladaná ako Analýza pomocou kontrolných záznamov využíva kontrolne záznamy krokov, podľa ktorých dochádza k overovaniu stavu prevádzky. Uvedené kontrolné záznamy obsahujú hodnotenie: „áno“, „nie“, „nie je vhodné“, „nie sú potrebné ďalšie informácie“ a dochádza k aplikovaniu do sektorov, kde dochádza ku kontrole súladu s predpismi a štandardami. Rutinné testy sú využívané v počiatočnom štádiu rozhodovacieho procesu, kedy dochádza ku overovaniu bezpečnosti vstupných materiálov a látok, ktoré majú byť v navrhovanom procese použité. Cieľom zistenia bezpečnosti pomocou metódy Čo sa stane ak, je identifikácia nebezpečných stavov v technologickom procese. Dochádza ku kladeniu otázok, pomocou ktorých sa zisťujú príčiny havárie a navrhujú sa opatrenia na zvýšenie bezpečnosti.

2.4.1 Analýza SWOT

SWOT analýza je považovaná za jeden z prvých analytických nástrojov používaných pre organizáciu. Názov „SWOT“ tvoria počiatočné písmená z anglických výrazov Strengths, Weaknesses, Opportunities, Threats. Analýza vychádza z princípu, že hodnotí vnútorné silné a slabé stránky a zároveň definuje externé, alebo vonkajšie príležitosti a hrozby. V ďalšom kroku dochádza ku komplexnému vyhodnoteniu situácie a definovaniu problému, alebo príležitosti.

	POMOCNÉ (k dosiahnutiu cieľa)	ŠKODLIVÉ (k dosiahnutiu cieľa)
Vnútročné (atribúty organizácie)	STRENGTHS (silné stránky) •	WEAKNESSES (slabé stránky) •
Vonkajšie (atribúty prostredia)	OPPORTUNITIES (príležitosti) •	THREATS (hrozby) •

Obr. 10. Definovanie analýzy SWOT [16]

Analýza SWOT v praktickom použití využíva následné hodnotenie pomocou váhy a hodnotenia. Pri hodnotení silných stránok a príležitostí dochádza k použitiu kladnej stupnice, a to napríklad v rozmedzí 1 až 5 s tým, že hodnota 5 reprezentuje najvyššiu spokojnosť a hodnota 1 najnižšiu spokojnosť. U slabých stránok a hrozieb dochádza k použitiu zápornej stupnice, a to napríklad od -1 do -5, kde -1 reprezentuje najnižšiu nespokojnosť a -5 najvyššiu nespokojnosť. Samotné hodnotenie jednotlivých položiek je veľmi komplikovaný proces, pri ktorom musí dochádzať k tomu, aby analytik zvažoval vzťah uvedenej položky vzhľadom na organizáciu. Váhou dochádza ku vyjadreniu dôležitosti jednotlivých položiek, ktoré sú prítomné v SWOT analýze. Dochádza k dodržiavaniu dvoch základných pravidiel, a to že súčet váh v danej kategórii musí byť rovný číselnej hodnote 1. Druhé pravidlo môžeme definovať, ako aspekt, že čím vyššie číslo má daná položka v danej kategórii, tým je daná položka dôležitejšia. [16]

Ďalší krok môže byť reprezentovaný, ako získanie prehľadu o postavení organizácie. Uvedený prehľad je väčšinou vykonávaný v ďalšom stĺpci danej analýzy, kde dochádza ku vynásobeniu váhy a hodnotenia danej položky. Následne dochádza ku sčítaniu daných hodnôt v danej kategórii, potom sčítaniu internej časti analýzy (slabé a silné stránky), sčítanie externej časti analýzy (príležitosti a hrozby) a na záver ku konečnej bilancii, počas ktorej dochádza ku odčítaniu príležitostí od hrozieb.

2.4.2 Úvodná analýza nebezpečenstva

Cieľom úvodnej analýzy nebezpečenstva (Preliminary Hazard Analysis) je poskytnúť vo veľmi krátkom časovom intervale prehľad prevádzkových nebezpečenstiev, ktorý je tiež

následne použitý na detailnú analýzu nebezpečenstva. Základnou myšlienkou PHA je zvoliť predmet štúdia a identifikovať, ktoré problémy môžu vzniknúť.

Pre použitie a aplikáciu danej analýzy platia nasledujúce zásady:

- Každé nebezpečenstvo je charakterizované relatívnou početnosťou, následkami a dochádza k identifikácii následných havárií.
- Každá zo zvolených havárií je odhadovaná pomocou predpokladanej početnosti a stupňa poškodenia zdravia jednotlivca, alebo skupiny.
- Uvedený odhad je určený len približne, a z uvedeného dôvodu sú početnosti a ich následky klasifikované len v určitých rozmedziach.

Tab. 2. Definovanie vzťahu medzi početnosťou a stupňom poškodenia zdravia [16]

Početnosť P		Stupeň poškodenia zdravia S	
K havárií nedôjde – nebezpečenstvo vylúčené	0	Bez zranenia	0
Menej ako 1x za 1000 rokov	1	Ľahké zranenia	4
Medzi 1x za 100 a 1x za 1000 rokov	2	Vážne zranenia	2
Medzi 1x za 10 a 1x za 100 rokov	3	Smrteľná nehoda	3
Medzi 1x za rok a 1x za 10 rokov	4	Niekoľko smrteľných nehôd	5
Častejšie ako 1x za rok	5		
Index rizika: I = P+ S			

Index rizika naznačuje závažnosť a následne je možné definovať, ktoré z analyzovaných rizík si vyžadujú zvláštnu pozornosť. Vo väčšine prípadoch dochádza ku určeniu rozsahu detailnejšej analýzy.

2.4.3 Štúdia nebezpečnosti a prevádzkyschopnosti

Jeden z najrozšírenejších prístupov k identifikácii nebezpečenstva je štúdia nebezpečenstva a prevádzkyschopnosti, ktorá je nazývaná aj HAZOP (Hazard and Operability Study). Pri aplikácii danej metódy do organizácie dochádza ku kritickému posúdeniu projektu, ku ktorému dochádza systematicky s využitím série kľúčových slov. Séria kľúčových slov sa použije systematicky, aby si členovia tímu mohli okamžite vytvoriť predstavu o identifikácii pravdepodobnosti odchýlky od navrhovaných podmienok. Jednou z ďalších podmienok je nutnosť určiť, či existuje podmienka, pri ktorej by mohlo dôjsť k odchýlke. Ak uvedená príčina existuje, je nutné skúmať dôsledky.

Relatívne jednoduchá aplikácia kľúčových slov NO, NOT, MORE, LESS predstavuje zreteľnú, jasnú a ľahko pochopiteľnú definíciu odchýlky. Kvalitatívny charakter majú kľúčové slová AS WELL AS, PART OF. Uvedené dva kľúčové slová by mali zachovávať svoj charakter a to na minimálne v čiastočnom znení. Kľúčové slovo REVERSE charakterizuje negáciu pôvodného účelu, a tým je jednoznačne vytvorená odchýlka. V prípade, že dochádza ku spojeniu časového údaju a kľúčových slov, potom MORE, LESS môžu byť definované, ako kratšia a dlhšia doba trvania, alebo tiež vyššiu alebo nižšiu početnosť. Ak definujeme časovú postupnosť, tak dochádza k používaniu špeciálnych kľúčových slov, a to SOONER (skôr, skorší), LATER (neskôr, neskorší).

Tab. 3. Definovanie kľúčových slov metódy analýzy rizík HAZOP[16]

Kľúčové slovo	Význam	Výklad
NO, NOT (žiadny, nie je)	kompletná negácia účelu	Nebola realizovaná žiadna časť účelu
MORE (viac, vyšší)	zvýšenie	Vzťahuje sa k množstvu a vlastnostiam, napr. rýchlosť prietoku, teplota apod., rovnako aj k činnostiam, napr. ohrev, reakcia atď.
LESS (menej, nižší)	kvantitatívne zníženie	Vzťahuje sa k množstvu a vlastnostiam, napr. rýchlosť prietoku, teplota apod., rovnako aj k činnostiam, napr. ohrev, reakcia atď.
AS WELL AS (takisto, tiež)	kvantitatívne zvýšenie	Všetky navrhnuté účely sú dosiahnuté spolu s určitou prídavnou činnosťou
PART OF (časť niečoho)	kvantitatívne zníženie	Realizované sú iba niektoré zámery (účely)
REVERSE (reverz, spätný)	logický protiklad	je najvhodnejší pre činnosti ako spätný tok alebo chemická reakcia, môže sa aplikovať aj vo vzťahu k látkam
OTHER THAN (iný než)	kompletná náhrada	Nedosiahla sa žiadna časť z pôvodného účelu, dochádza k inej činnosti

2.4.4 Analýza vplyvov porúch a ich následkov

Analýza vplyvov porúch a ich následkov (FMEA – Failure Modes and Effects Analysis) hodnotí možné poruchy zariadenia a ich vplyvy na technologický proces, ku ktorým môže dôjsť na rôznych úrovniach – v systéme, subsysteme, alebo jeho komponentoch. Môže dôjsť ku rozšíreniu o početnosť výskytu porúch, alebo o ich pravdepodobnosť.

V uvedenom prípade sa realizuje Failure Modes, Effects and Criticality Analysis – FMECA. [16]

FMEA je jedným z prvých systematických postupov pre analýzu porúch, ktorý skúma každý komponent systému, a to kladením nasledujúcich otázok:

- Ako sa môže komponent poškodiť?
- Čo sa môže stať keď sa komponent poškodí?

FMEA je pomôckou v celkovej analýze rizika, výsledky sú spracované pomocou tabuliek, pričom sú volené rôzne formy záznamu. Záverečnú etapu tvorí štúdium kritickosti porúch, pričom dochádza k výberu porúch, ktoré sú najzávažnejšie. Nasledujúca tabuľka popisuje kategórie kritickosti.

Tab. 4. Kategórie kritickosti metódy analýzy rizík FMEA[16]

Kategória	Následky
Katastrofická	strata systému (zariadenia), niekoľkonásobné zranenie, smrť
Kritická	zranenie, poškodenie zariadenia, nebezpečný stav vyžadujúci okamžitú nápravu
Okrajová	žiadny dôležitý systém nie je poškodený, žiadne poškodenie funkcie zariadenia, žiadne zranenie osôb
Zanedbateľná	žiadny dôležitý systém nie je poškodený, žiadne zranenie osôb, nie je potrebná okamžitá náprava

Aby metóda FMEA bola úspešná, je nutné dbať na dobrú koncepciu odhadu, ktorá definuje poruchy vyskytujúce sa vo výrobnom procese, na výrobnom zariadení a aké príčiny ich spôsobujú.

2.4.5 Analýza stromom porúch

Analýza stromom porúch (Fault Tree Analysis – FTA) je založená na zostavení schémy porúch. Strom porúch má tzv. „TOP“ udalosť, ktorá prezentuje vrcholnú časť a predstavuje hlavnú nežiaducu udalosť. V spojení s uvedenou udalosťou je možné použiť OR GATE, ktorý definuje niekoľko vstupných možností, následne uvedené možnosti špecifikuje, či definovaná výstupná udalosť môže nastať, za prítomnosti akejkoľvek z vstupných možností.

Použitie AND GATE vyjadruje, že výstupná udalosť nastane iba v prípade, ak sa vyskytnú všetky vstupné možnosti. [16]

Analýzou pomocou stromu porúch dochádza k vytvoreniu systematického vizuálneho zobrazenia, ktoré definuje, akým spôsobom prispievajú jednotlivé príčiny prvkov k poruchovosti systému.

2.4.6 Analýza stromom nebezpečenstva

Analýza stromom nebezpečenstva (Hazard Tree Analysis - HTA) je primárne postavená na zásade voľby typu havárie, ktorá postačuje na pokrytie daných riešených problémov. Uvedené typy havárií sú roztriedené a v počiatočnom štádiu sú analyzované.

Podtriedy typu havária musia spĺňať nasledujúce podmienky:

- Vzájomne by sa mali jednotlivé typy havárií vylučovať,
- Jednotlivé typy havárií by mali byť na každej úrovni približne rovnako vyznačené,
- Havárie by mali mať úplný logický dosah pôsobnosti.

Nasledujúce kroky popisujú postup pri zostavovaní stromu nebezpečenstva:

1. Voľba vhodnej hlavnej udalosti (havária),
2. Zostavenie záznamu druhov príčiny pre vrcholnú udalosť (môže dôjsť k použitiu kontrolného záznamu),
3. Pripojenie zistených druhov príčin, a to na pozíciu vstupných údajov k hodnoteniu poruchovej schémy,
4. Pochopenie každého druhu nebezpečenstva a detailné rozvinutie príčiny, a to pomocou ďalších krokov.

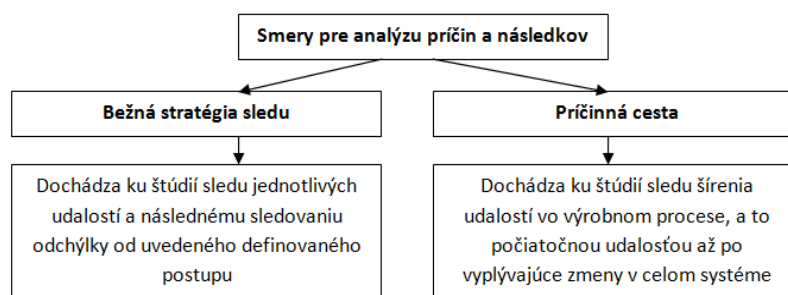
Analytickú metódu stromu nebezpečenstva (HTA) je možné kombinovať s analytickou metódou stromom porúch (FTA), a to zvyčajne za účelom vypracovania analýzy príčin následkov (CCA). [16]

2.4.7 Analýza príčin následkov

Analýza príčin následkov (Cause Consequence Analysis – CCA) je definovaná, ako pracovný postup, ktorý v prvotnej fáze zahrňuje skúmanie počiatočnej „ rozhodujúcej udalosti“, a v nasledujúcej fáze dochádza ku štúdiu sledu jednotlivých udalostí

v konkrétnom procese s ohľadom na príčiny. Diagram príčin a následkov vizualizuje výsledky analýzy, a to s preferenciou príčinného vzťahu medzi udalosťami a časovým intervalom. V prípade analýzy dochádza ku sledovaniu reťazcov udalostí a dochádza taktiež ku rozdeleniu uvedeného reťazca na alternatívne a paralelné vetvy, ktoré prispievajú k lepšiemu vysvetleniu príčiny pomocou použitia malého stromu porúch.

Analýza príčin následkov vychádza z rozhodujúcej udalosti, ktorá je často označovaná za kritickú udalosť. Kritickú udalosť definujeme, ako udalosť, ktorá za určitých okolností môže spôsobiť závažné následky a zároveň je vhodnou na použitie počiatočnej udalosti pre vypracovanie analýzy. Pri voľbe rozhodujúcej udalosti by sme mali dohliadať na dôležitý vplyv časového sledu, a to z dôvodu jednoduchšieho spracovania. Najdôležitejšie prípady porúch by mali byť definované, ako rozhodujúce udalosti, a teda by malo dochádzať ku pokrytiu nebezpečenstva zariadenia.



Obr. 11. Definovanie primárnych smerov analýzy príčin a následkov [16]

Uvedené smery stratégie je možné aplikovať pre všetky prítomné stavy v danej prevádzke, pre bežnú prevádzku, zníženú výrobu, ale aj pre nenominálne prevádzkové stavy. Bežná stratégia sledu je vhodná predovšetkým pre diskontinuálne procesy, pričom práve príčinná cesta je najvhodnejším riešením pre kontinuálny proces.

2.4.8 Analýza spoľahlivosti človeka

Analýza spoľahlivosti človeka (Human Reliability Analysis – HRA) je cielená na identifikáciu ľudských chýb a vzájomné pôsobenie na príčiny uvedených chýb. Uvedenú analýzu môžeme definovať, ako systematické hodnotenie faktorov, ktoré ovplyvňujú ľudskú činnosť. Uvedený typ analýzy je veľmi dôležitý hlavne v systémoch, ktoré by mohli byť významne ovplyvnené chybou človeka, a teda mohlo by dochádzať k návrhu pred opatrení, ktoré znižujú riziko vzniku uvedených udalostí. [16]

2.4.9 Paretova analýza

Paretova analýza, dosť často označovaná aj ako ABC analýza, vychádza z Paretovho pravidla, ktoré definuje, že 20% činnosti produkuje 80% následku. Uvedené pravidlo je vyjadrované ako nelineárna závislosť, ktorá sa prejavuje vo všetkých oblastiach ľudskej činnosti. Práve Paretova analýza má za cieľ zistiť, ktoré udalosti spôsobujú definovaný problém. V dnešnej dobe je uvedený druh analýzy používaný pre veľké spektrum odvetví. Je nutné ale poznamenať, že aj 20% príčin bude mať významný následok. V prípade rozdelenia do kategórií A, B a C sú uvedené kategórie definované nasledovným spôsobom:

- Kategória A – zaradené príčiny, ktoré spôsobujú 80% následkov,
- Kategória B – zaradené príčiny, ktoré spôsobujú 10- 15% následkov,
- Kategória C – dochádza k zaradeniu ostatných príčin.

Vizualizácia Paretovej analýzy je realizovaná pomocou Lorenzovej krivky, ale v praxi dochádza k viacerým grafickým vizualizáciám. Uvedený typ analýzy prebieha z dôvodu, aby došlo k odhaleniu väčšinových spôsobovaných následkov, ale musíme poukázať aj na to, že aj keď odhalíme daných 20% príčin, ktoré spôsobujú 80% negatívneho pôsobenia, a teda aplikovaním nápravného riešenia znížime negatívne pôsobenie, stále je v danom procese prítomná možnosť, že aj iná príčina môže byť významným činiteľom. Je nutné dohliadať na systém analýzy, a teda dodávať analýze extrémnu pozornosť. [16]

2.4.10 Krízová matica

Krízová matica je jeden z analytických spôsobov, ktorý zahrňuje v svojej podstate aj vyhodnotenie rizík. Winterlingova krízová matica používa pre analytické hodnotenie dva parametre kategórie rizík. Prvý parameter je pravdepodobnosť vzniku rizika v reálnom časovom intervale a druhý parameter je definovanie závažnosti nehody, alebo danej udalosti.

[16]

Pravdepodobnosť vzniku udalosti v danom časovom intervale	Závažnosť nehody alebo udalosti			
		<i>negatívne</i>	<i>ohrozujúce</i>	<i>zničujúce</i>
	<i>vysoká</i>	3	4	5
	<i>stredná</i>	2	3	4
<i>nízka</i>	1	2	3	

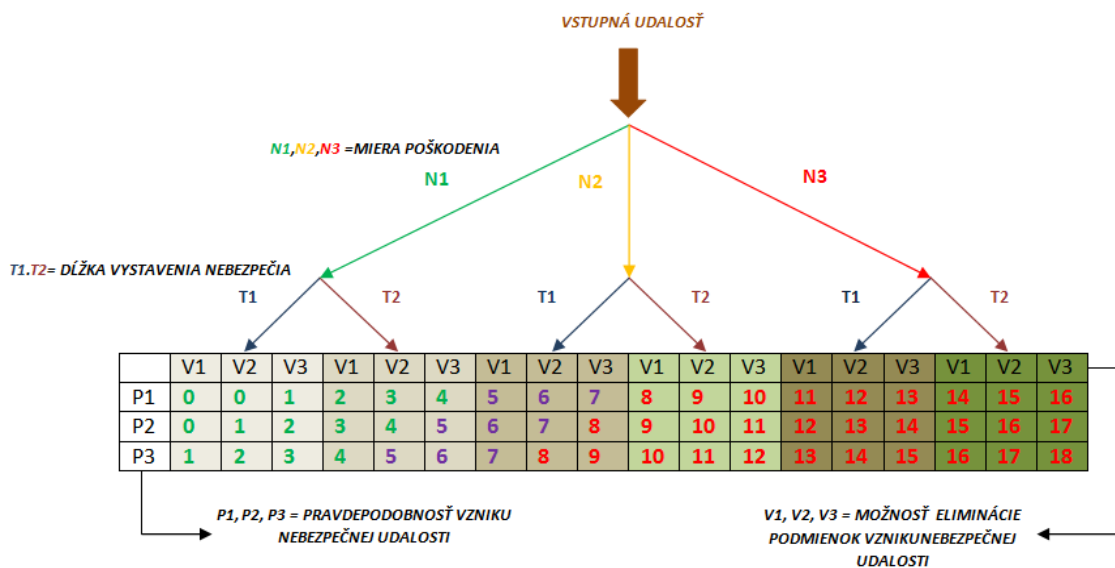
Obr. 12. Vzor aplikácie analytického vyhodnotenia pomocou krízovej matice

ZDROJ: (autor)

Definovanie intervalu hodnotenia miery rizika upravuje samotný analytik podľa potreby samotnej analýzy. Výstupom hodnotenia dochádza k nastaveniu intervalu, a to napríklad:

- interval $\langle 1;2 \rangle$ - hodnota rizika je prijateľná,
- interval $\langle 3;4 \rangle$ - hodnota rizika je neprijateľná,
- interval $\langle 4;5 \rangle$ - hodnota rizika je vyslovene neakceptovateľná.

V prípade, že používame vyššiu úroveň analýzy je nutné zvoliť prijateľný spôsob hodnotenia, a to napríklad určovanie desatinných miest, alebo zaznamenávanie pomocou charakteristických bodov a následne definovať vyhodnocovací proces pre danú metódu. Nevýhodou danej analýzy je použitie dvoch parametrov na hodnotenia. Avšak uvedenú nevýhodu odstránime spracovaním maticovej metódy pre odhad rizika, ktorá je založená na hodnotení a posúdení viacerých parametrov, ktorými sú napríklad poškodenie, dĺžka vystavenia nebezpečenstvu, možnosť vyvarovania sa nebezpečenstvu a pravdepodobnosť vzniku nebezpečnej udalosti. Na základe určenia uvedených hodnôt sa postupuje smerom, ktorý určujú šípky, a to až ku hodnote prijateľného rizika. Pre každé identifikované nebezpečenstvo, alebo danú udalosť sa stanovuje odhad rizika zvlášť. Výsledkom je hodnota, ktorá definuje prijateľnosť rizika. Ak je uvedená zistená hodnota príliš veľká, dochádza k návrhu a aplikácii bezpečnostných opatrení, a teda by malo dôjsť k zníženiu danej hodnoty pri prepočítaní. Ak zistená hodnota spadá do intervalu prijateľného rizika, definujeme daný stav, ako prítomné zostatkové riziko.



VYHODNOTENIE PRIJATEĽNOSTI RIZIKA:

0 – 4 = AKCEPTOVATEĽNÉ RIZIKO
 5 - 7 = PO PREVERENÍ AKCEPTOVATEĽNÉ RIZIKO
 7 – 18 = NEAKCEPTOVATEĽNÉ RIZIKO

Obr. 13. Vzorové spracovanie maticovej metódy vyhodnotenia rizika

ZDROJ: (autor)

Závažný faktor pri procese posudzovania rizika je skutočnosť, ako je dané riziko prijímané. Dobrovoľné prijatie rizika jedincou, alebo organizáciou, je riziko, o ktorom je daný subjekt informovaný a je možné jeho pravdepodobnosť vzniku ovplyvniť, a to aplikáciou správne definovaných postupov, teda je možné, aby sa daný subjekt eliminačnými postupmi vyhol možnosti vzniku krízovej udalosti.

2.5 Bezpečnostné opatrenie pre minimalizovanie rizika v organizácií

Uvedená časť práce definuje základné spôsoby, ktoré sú aplikované do organizácie, ako súčasť bezpečnostnej politiky, a to za cieľom minimalizovať definované riziko, ktoré bolo vyhodnotené analytickým procesom. Je možné uvedené opatrenia klasifikovať, ako metódy prístupu, ktoré za určitých podmienok, väčšinou určené plánom v čase, dosiahnu definované zníženie rizika.

2.5.1 Definovanie fyzickej bezpečnosti organizácie

Definovanie fyzickej bezpečnosti organizácie pozostáva z definovania základných technických komponentov, ktoré sú účelne navrhnuté na zabezpečenie fyzickej bezpečnosti objektov organizácie.

Fyzická bezpečnosť objektov je realizovaná:

- Smernicou fyzickej bezpečnosti, ktorá definuje požiadavky,
- Mechanickými zábrannými systémami,
- Poplachovými a zabezpečovacími tiesňovými prvkami,
- Kamerovým systémom,
- Prístupovým systémom.

2.5.2 Režimové opatrenia

Režimová ochrana definuje spôsoby, akými by mali osoby nachádzajúce sa v organizácii postupovať pri ochrane podniku. Dochádza k definovaniu režimu, ktorý má byť dodržaný v jednotlivých funkciách, alebo v definovaných podmienkach. Je nutné pri definovaní uvedených opatrení vychádzať zo základných a prioritných zákonov Českej republiky, ktoré definujú, že nezadané ľudské práva a slobody môžu byť obmedzené len na základe zákona a zákonných dôvodov, ktoré sú stanovené zákonom. Režim je definovaný, ako administratívne, organizačné a vecné usporiadanie vzťahov medzi ľuďmi, ich činnosťami a procesmi v oblasti výkonu a riadenia, a to za účelom zladenia všetkých prvkov s cieľom dosiahnuť harmonický stav v danej organizácii. [12]

Režimové opatrenia definujú:

- Činnosť zamestnancov v internom prostredí podniku,
- Pohyb a chovanie sa cudzích osôb prichádzajúcich z externého prostredia do organizácie,
- Výstup informácií z interného prostredia do externého prostredia (práca s dokumentmi).

ZDROJ: [12]

2.5.3 Definovanie bezpečnostnej dokumentácie

Definovaním bezpečnostnej dokumentácie dochádza ku konkrétnej realizácii pravidiel definovaných bezpečnostnou politikou organizácie. V prípade, že dôjde k definovaniu internej legislatívy vzťahujúcej sa k bezpečnosti organizácie, jedná sa o najefektívnejší spôsob pre presadenie stanovených cieľov. Prevádzacie dokumenty sú stanovené vo forme interných smerníc, nariadení, pokynov, popisov funkčných a pracovných postupov. V prípade definovania uvedených dokumentov musí dôjsť k stanoveniu kompetencií, ktorými sú definované povinnosti a zodpovednosti jednotlivých zamestnancov podniku, alebo organizácie. V uvedených dokumentoch sú primárne uvedené postupy, ktorými by malo dôjsť k prevencii pred určitými rizikami a hrozbami. [12]

Potrebné dokumentáciou určiť:

- Kto má čo robiť,
- Definovať, čo má robiť,
- Časový plán, kedy má danú činnosť robiť,
- Spôsob, akým to má urobiť.

ZDROJ: [12]

Bezpečnostná dokumentácia pojednáva o preventívnych opatreniach, ktorými sú napríklad plány pre pracovnú činnosť, plány pre minimalizovanie rizika, a iné dokumenty, ktorých použitím v procese dôjde k minimalizovaniu možnosti vzniku nežiaducej udalosti. Medzi ďalšie patria dokumenty, ktoré definujú, ako majú byť jednotlivé postupy kontrolované a súčasne v akých intervaloch má ku kontrole dochádzať, a akým spôsobom má byť kontrola hodnotená. Súčasťou bezpečnostnej dokumentácie sú aj technické výkresy, ktoré definujú rozloženie kancelárskych priestorov, ale aj inštalovanie jednotlivých komponentov. Technické výkresy môžu slúžiť aj ako vstup pre definovanie režimových opatrení.

2.5.4 Školiace procesy

Definovaním a plánovaním školení v jednotlivých odvetviach dochádza ku oboznámeniu a vysvetleniu uvedených smerníc pre zamestnancov, čo následne môže viesť k aplikácii daných smerníc do prevádzkových činností. Z uvedeného dôvodu, by pri definovaní bezpečnostných pravidiel malo dochádzať ku plánovaniu školení v oblasti bezpečnosti. Je to

jednoduchý proces, kedy v prípade, že dôjde ku definovaniu pravidiel, aj k ich zavedeniu do interných smerníc, ale daný zamestnanci nepochopili účel, a teda nedochádza k adekvátnemu použitiu smerníc v pracovnom prostredí, tak nebude naplnený cieľ minimalizovania rizika a iniciatíva tvorby plánu je zbytočná. Je preto nevyhnutné dbať na pochopenie jednotlivých pravidiel osobami, ktoré dané pravidlá majú rešpektovať a zavádzať do procesu.

2.5.5 Nastavenie riadenia

Pre plnenie bezpečnostných pravidiel, by mal bezpečnostný projekt pojednávať o riadení podniku, ale aj o riadení v prípade bezpečnostného incidentu. Malo by byť určené krízové riadenie, teda vedenie, ktoré bude ovládať podrobný proces riadenia bezpečnostného incidentu a pravidelne sa bude zúčastňovať jednaní, ktoré budú aktualizovať bezpečnostný projekt, aby bol v dobe účinný.

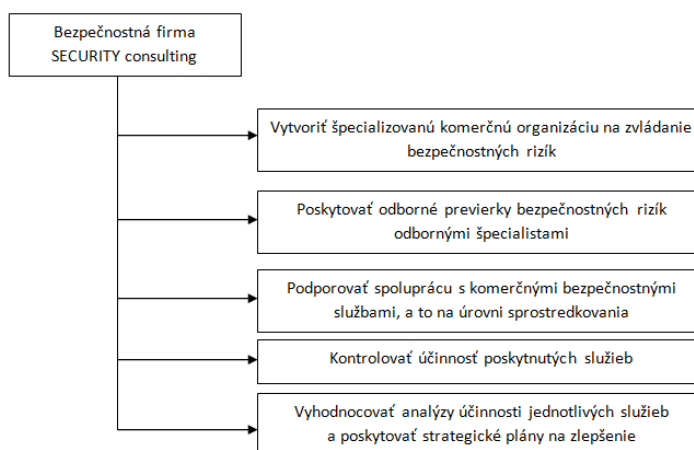
Teoretická časť práce popisovala základné princípy bezpečnostnej politiky, pričom dochádzalo ku teoretickému uvedeniu jednotlivých postupov a analytických metód. V závere časti práce došlo ku uvedeniu opatrení využiteľných na minimalizáciu vzniku rizika. Z hľadiska právnych predpisov dochádzalo ku uvedeniu základných právnych vzťahov, ktoré sa dotýkajú problematiky bezpečnostnej politiky. Uvedená časť práce definovala teoretický základ pre vykonanie praktickej časti, kde dochádza ku aplikovaniu zistených poznatkov do procesu stanovovania bezpečnostnej politiky organizácie, ktorá je popisovaná v úvode praktickej časti.

II. PRAKTICKÁ ČASŤ

3 INFORMÁCIE O SPOLOČNOSTI

V praktickej časti práce dochádza k použitiu teoretických poznatkov v praktickom využití vybranej spoločnosti. Aplikáciou jednotlivých metód na fungujúci systém spoločnosti bude dochádzať ku zhodnoteniu súčasnej situácie a následné určenie bezpečnostných opatrení, ktoré svojou účinnosťou budú vytvárať kontext bezpečnostnej politiky daného podniku.

Pre praktickú časť práce bola zvolená organizácia zaoberajúca sa poskytovaním bezpečnostných služieb v komerčnej oblasti pôsobenia. Základným cieľom organizácie je vytvoriť systém bezpečnostných služieb na profesionálnej úrovni, a teda vystupovať ako jediný dostupný prostriedok na zhodnotenie súčasne poskytovaných služieb v oblasti komerčnej bezpečnosti, a tým dosiahnuť požadovanú úroveň zákazníka.



Obr. 14. Primárne ciele organizácie

ZDROJ: (autor)

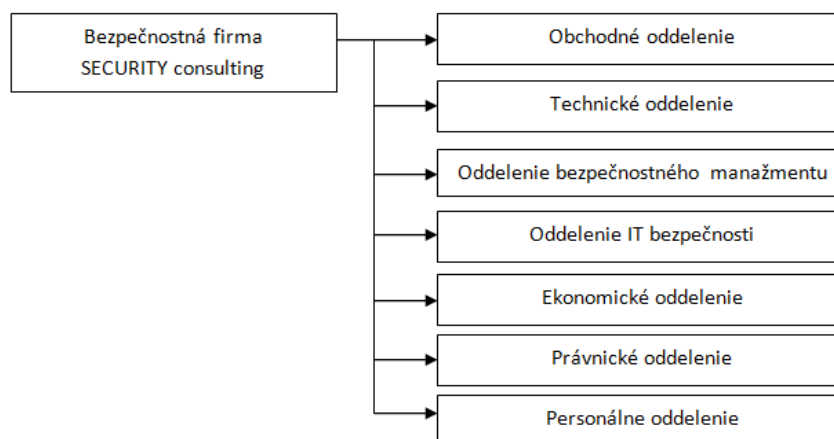
Primárne ciele organizácie popisujú základné ciele, ktoré charakterizujú pôsobenie organizácie do budúceho vývoja. Uvedené ciele sú reprezentované jednotlivými oddeleniami a činnosťou jednotlivých pracovníkov v jednotlivých odvetviach bezpečnostných služieb.

V súčasnej dobe dochádza k najvyššej produktivite v oblasti poskytovania fyzickej ochrany majetku a zabezpečovanie súkromných akcií, ale aj verejných podujatí. Cieľ organizácie je vytvoriť bezpečnostnú organizáciu, ktorá na základe skúseností a poznatkov vytvorí systém celkovej ochrany pre zákazníka, a to tým spôsobom, že jednotlivé odvetvia budú zastupovať kvalifikovaní odborníci na riešenie daných problémov. Cieľ analyzovanej organizácie je bezpečnostný, a teda pri návrhu bezpečnostnej politiky musia byť skúmané konkrétne ciele tak, aby dochádzalo k vytvoreniu optimálneho klimatického prostredia pre

aplikáciu určitých funkcií organizácie. Každá poskytovaná služba musí byť poskytovaná tak, aby dochádzalo ku najvyššej účinnosti u klienta, tým pádom musí byť danou službou znížené riziko na najmenšiu prijateľnú úroveň a zároveň musí dochádzať k ochrane organizácie samotnej. Ak uvedená organizácia, alebo spoločnosť má za cieľ poskytovať kvalitné bezpečnostné služby musí primárne dokázať ochrániť a zabezpečiť firemnú bezpečnosť.

3.1 Charakteristická štruktúra podniku

Štruktúra organizácia je definovaná základnou myšlienkou, ako by uvedená organizácia mala byť plne funkčná a malo by dochádzať k naplneniu vytýčených cieľov s minimalizáciou straty. V súčasnej dobe nedochádza ku naplneniu všetkých vytýčených cieľov organizácie, ale práve preto aj navrhnutím bezpečnostnej politiky by malo dôjsť k zníženiu miery neúčinnosti jednotlivých služieb.



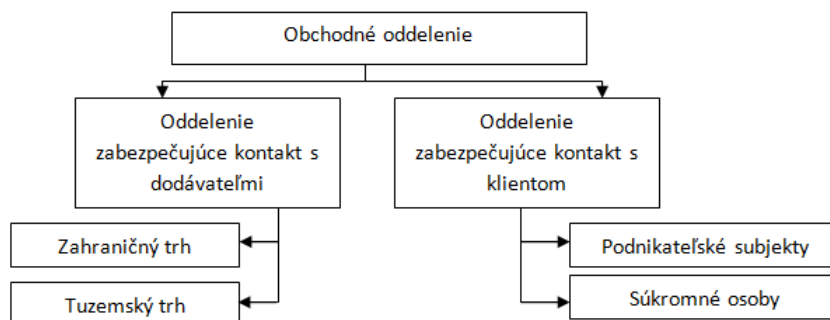
Obr. 15. Základné rozdelenie spoločnosti

ZDROJ: (autor)

Základné rozdelenie spoločnosti definuje primárne oddelenia, ktoré sú charakteristické odvetvím, ktorým sa zaoberajú jednotliví pracovníci a spoločne by malo dochádzať k naplneniu cieľu organizácie. Sub cieľom bezpečnostnej politiky bude zvýšiť produktivitu oddelení, a to z dôvodu, že v súčasnosti nie sú plne funkčné všetky väzby prítomné v organizácií.

3.1.1 Obchodné oddelenie podniku

Nasledujúca kapitola práce charakterizuje definované ciele spoločnosti a stav, kam by mal podnik postupovať. Dochádza ku definovaniu primárneho účelu obchodného oddelenia.



Obr. 16. Základné zobrazenie funkcií obchodného oddelenia

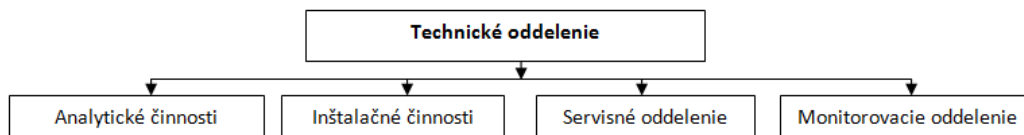
ZDROJ: (autor)

Cieľom obchodného oddelenia spoločnosti je zaistiť komunikáciu s klientom a dodávateľmi. Medzi dodávateľské kontakty patria technické spoločnosti, ktoré dodávajú technické komponenty na realizáciu ochrany majetku, a teda prevažne dodávajú komponenty elektronickej požiarnej signalizácie, elektronických zábranných systémov, mechanické zábranné prvky, ale aj kamerové jednotky a softvér na podporu riadenia a iné prostriedky a nástroje, ktoré spoločnosť následne nasadzuje do jednotlivých projektov. Obchodné oddelenie zabezpečuje vzájomné vzťahy na zahraničnej, ale aj tuzemskej úrovni pôsobenia. Súčasne dochádza k riešeniu obchodných prípadov s klientmi, alebo potenciálnymi zákazníkmi, ktorí potrebujú jednorazové služby, alebo sa jedná o dlhodobý proces poskytovania jednotlivých služieb, ktoré majú medzi sebou navzájom vytvorené väzby, a tým dochádza k naplneniu primárnej požiadavky klienta.

3.1.2 Technické oddelenie podniku

Nasledujúca časť práce definuje technické oddelenie spoločnosti. Technické oddelenie spoločnosti je v súčasnosti neúčinné a jednotlivé funkcie nenapĺňujú svoj účel. V súčasnej dobe technické oddelenie funguje podľa potreby klientov, ktoré nie sú predvídané a teda ich vykonávanie nie je dostatočne odborné. Z uvedeného dôvodu nasledujúci obrázok definuje primárne ciele technického oddelenia, a teda dochádza ku stanoveniu jednotlivých funkcií, ktoré by mali byť vytýčené pred samotným návrhom opatrení bezpečnostnej politiky, ktoré

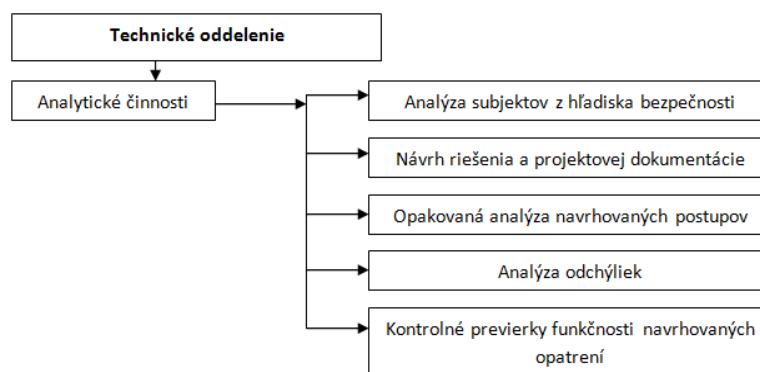
by malo zvýšiť prestíž a funkcionality celej firmy, ktorá sa zaoberá poskytovaním technických bezpečnostných služieb.



Obr. 17. Základné definovanie technického oddelenia

ZDROJ: (autor)

Jednotlivé sub oddelenia definujú činnosti, ktoré sú následne špecializované na konkrétne poskytované služby jednotlivými pracovníkmi. V prvej fáze technického poskytnutia služby je analýza stavu, ktorá je následne vyhodnotená a dochádza k navrhnutiu technického riešenia a inštalácií systému. Inštalovaný systém je po určitej časovej perióde servisovaný a následne aktualizovaný do prevádzkového stavu, ktorý splňuje požiadavky daného prostredia. Monitorovacie činnosti zabezpečujú monitoring v uvedených objektoch, a tým dochádza ku naplneniu funkcií technických komponentov, ktoré v predchádzajúcej fáze boli zavedené do prevádzky.

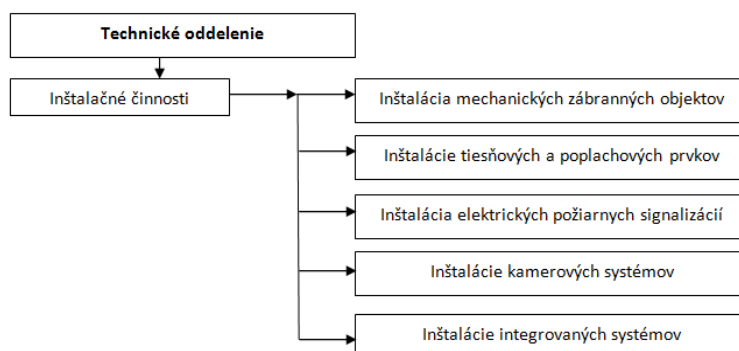


Obr. 18. Definovanie analytickej činnosti technického oddelenia

ZDROJ: (autor)

Inštalčné činnosti technického oddelenia sú charakterizované inštaláciou jednotlivých technických komponentov, ktoré v spojení do jedného celku zabezpečujú funkčnosť navrhovaných projektov pre daného klienta. Pri zavádzaní jednotlivých komponentov musí dochádzať k dodržaniu pravidiel projektovej dokumentácie, aby nedochádzalo ku znehodnoteniu funkčnosti navrhovaných opatrení. Vzájomné väzby by mali byť dodržiavané

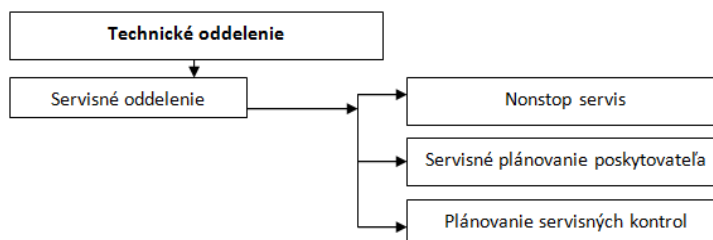
aj pri vzájomnej komunikácii a ovplyvňovaní systémov medzi sebou, a to z dôvodu, že vo viacerých projektoch dochádza k prepojeniu systémov.



Obr. 19. Definovanie inštalačných činností technického oddelenia

ZDROJ: (autor)

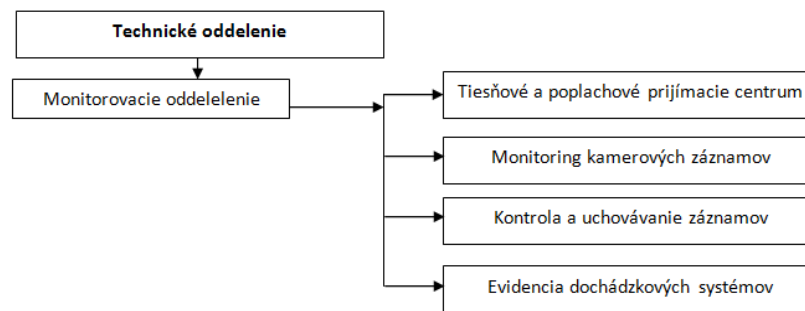
Servisné oddelenie má za hlavnú úlohu zabezpečovať pravidelný servis, ale aj mimoriadny servis, kedy by mala byť odstránená porucha systému v čo najkratšom časovom intervale a systém by mal byť obnovený do stavu prevádzky schopný, a teda by malo dochádzať k naplneniu úlohy bezpečnosti.



Obr. 20. Definovanie činností servisu technického oddelenia

ZDROJ: (autor)

Monitorovacia časť technického oddelenia má za hlavný cieľ zabezpečiť monitoring udalostí, ktoré sú monitorované pomocou technických komponentov a softvérového vybavenia jednotlivých objektov. V uvedenej časti technického oddelenia dochádza ku vyhodnocovaniu vzniknutých udalostí a kontrole požadovaného stavu uvedeného objektu. Taktiež dochádza k hodnoteniu celých aplikácií a externému vyhodnocovaniu evidencie jednotlivých procesov prítomných osôb v objekte, ktoré sú podľa potrieb klienta analyzované.



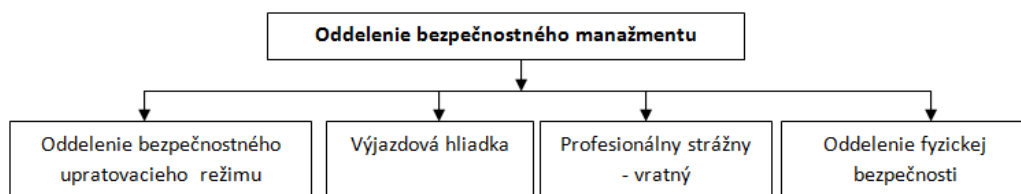
Obr. 21. Definovanie monitorovacích funkcií technického oddelenia

ZDROJ: (autor)

Zaručeniu najvyššej efektivity technického oddelenia je možné dosiahnuť v prípade, že jednotlivé sub oddelenia medzi sebou spolupracujú, a to z dôvodu, že jednotlivé funkcie na seba nadväzujú a jedna funkcia bez druhej nemá opodstatnené plnenie cieľu hlavne v oblasti bezpečnostnej firmy.

3.1.3 Oddelenie bezpečnostného manažmentu

Oddelenie bezpečnostného manažmentu by malo riešiť dohľad a realizáciu nad aplikovaním personálneho zabezpečenia jednotlivých projektov. Medzi bezpečnostné riadenie manažmentu patria personálne vykonávanie dopredu určených procesov, pri ktorých dochádza ku dôrazu na precíznosť a bezchybnosť vykonania jednotlivých funkcií.



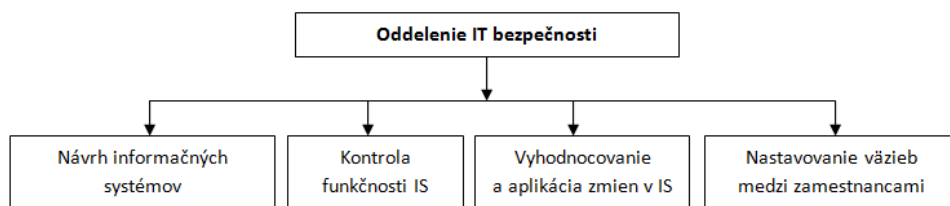
Obr. 22. Charakteristika oddelenia bezpečnostného manažmentu

ZDROJ: (autor)

3.1.4 Oddelenie bezpečnosti informačných technológií

Oddelenie bezpečnosti informačných technológií je možné charakterizovať, ako základný pilier práce s informáciami. V rámci uvedenej spoločnosti je nutné definovať pravidlá, podľa ktorých bude dochádzať k manipuláciám s dátami spoločnosti, ktoré sa dotýkajú interných

záležitostí spoločnosti. Vzhľadom na charakter uvedenej spoločnosti sú spracovávané dáta o klientoch a objektoch, ktoré sú predmetom ochrany veľmi citlivé vzhľadom ku majiteľovi.

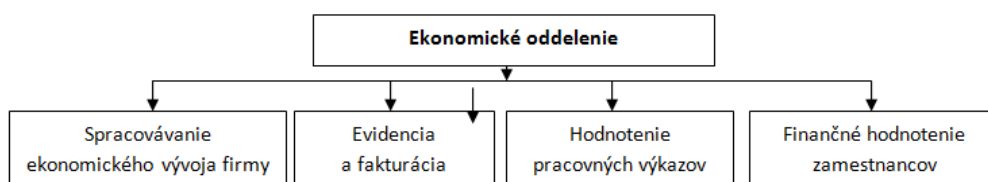


Obr. 23. Charakteristika oddelenia informačnej bezpečnosti

ZDROJ: (autor)

V súčasnosti uvedené oddelenie nie je plne funkčné, ale dochádza k obecnému naplneniu cieľa ochrany dát. Uvedená charakteristika oddelenia by mala byť vzorovou pre budúci vývoj spoločnosti. Spoločnosť chce realizovať aplikácie informačných systémov do iných podnikateľských subjektov, a to za cieľom ochrániť dáta spoločnosti, a tým prispieť k zvýšeniu efektivity bezpečnostných opatrení. Pri realizácii sa jedná primárne o vytvorenie dochádzkových systémov a systému na kontrolu práce a dát zamestnancov, ktoré nie sú prístupné pre tretie strany.

3.1.5 Ekonomické oddelenie organizácie



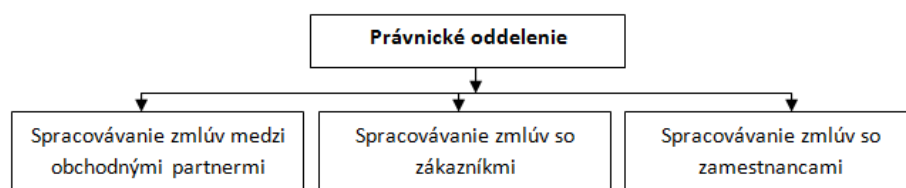
Obr. 24. Charakteristika ekonomického oddelenia

ZDROJ: (autor)

Ekonomické oddelenie spracováva štatistik o ekonomickom vývoji firmy, ale dochádza k tvorbe a evidencii fakturačných dokumentov, ale aj k hodnoteniu pracovných výkazov, a tým spojené finančné hodnotenie zamestnancov podľa dopredu určených štandardov firmy, ktoré sú zmluvne dohodnuté zo zamestnancami spoločnosti. V uvedenom procese je nutná spolupráca s právnym oddelením, ktoré vykazuje jednotlivé sadzby na ohodnotenie vykonanej práce.

3.1.6 Právnické oddelenie organizácie

Právnické oddelenie je primárnym oddelením, ktorého funkčnosť vedenie spoločnosti hodnotí veľmi kladne, a to hlavne z dôvodu, že sa v danom oddelení definujú zmluvné vzťahy s obchodnými partnermi, ale aj so zákazníkmi a v neposlednom rade so zamestnancami spoločnosti. Úzka spolupráca právneho oddelenia je hlavne z obchodným a ekonomickým oddelením. Obchodné oddelenie musí spolupracovať tak z treťou stranou, ktorú reprezentujú klienti, iné spoločnosti, partneri a iné subjekty, ako aj s uvedeným právnym oddelením.

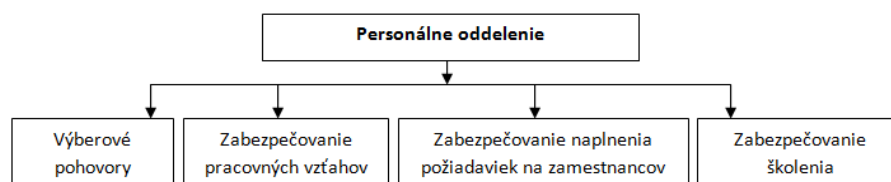


Obr. 25. Charakteristika funkcií právneho oddelenia

ZDROJ: (autor)

3.1.7 Personálne oddelenie organizácie

Personálne oddelenie realizuje svoju činnosť na pozícií výberových riadení na zamestnancov firmy, ktorých počet je dostatočne veľký vzhľadom ku bezpečnostným službám, ktoré firma poskytuje na úrovni bezpečnostných pracovníkov. Uvedené oddelenie zabezpečuje naplnenie legislatívnych požiadaviek na pracovné vzťahy. Jedným z ďalších úloh uvedeného oddelenia je zabezpečovať potrebné školenia pre zamestnancov, a tým prispievať k zvyšovaniu práce efektivity celej spoločnosti. Uvedené oddelenie úzko spolupracuje s technickým, ale aj právnym oddelením, a to hlavne v zaisťovaní pracovných zmlúv.

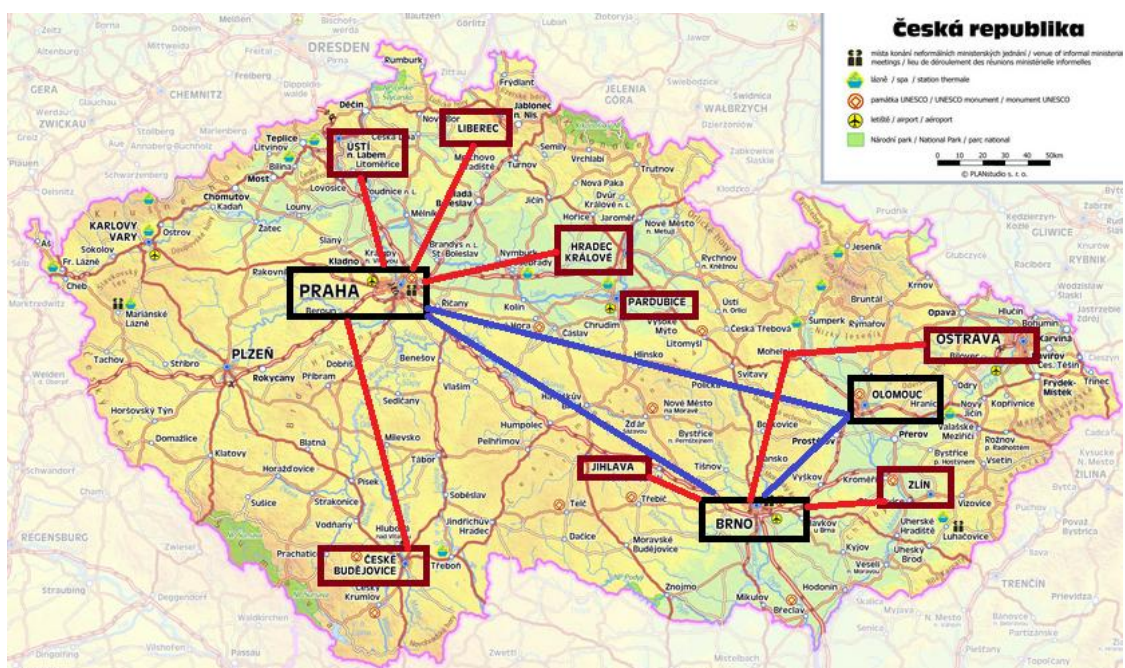


Obr. 26. Charakteristika funkcií personálneho oddelenia

ZDROJ: (autor)

3.2 Lokalizácia organizácie

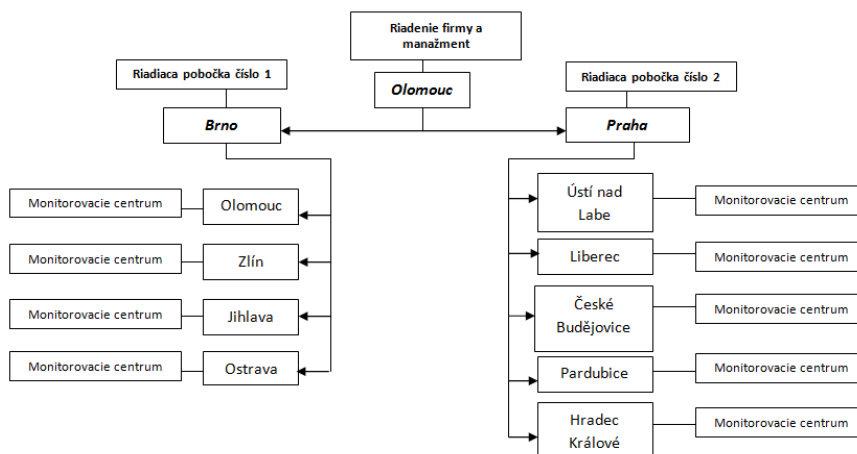
Uvedená kapitola sa zaoberá lokalizáciou sídla firmy, ale aj jednotlivých pobočiek, na ktorých dochádza k procesom sub riadenia jednotlivých služieb, ktoré sú klientom poskytované. Podnik má rozšírené svoje pobočky po Českej republike, ale taktiež dochádza ku manažovaniu jednotlivých pracovníkov, ktorý vykonávajú bezpečnostné funkcie u klientskej firmy, a to za pomoci okresných manažérov danej lokality. Lokalizácia je zobrazená na nasledujúcom obrázku, kde je primárne určená hierarchia jednotlivých pobočiek.



Obr. 27. Lokalizácia jednotlivých monitorovacích miest a pôsobnosti spoločnosti

ZDROJ: <http://www.eu2009.cz/cz/czech-republic/ceska-republika-376/>

Na zobrazenom obrázku číslo 9 dochádza k lokalizácií jednotlivých monitorovacích miest v Českej republike. Riadenie spoločnosti a manažment podniku je zabezpečovaný z lokality Olomouc. Štruktúra sa následne delí na dve sekundárne riadiace pobočky, ktoré sú sústredené do miest Brno a Praha. Pracovné náplne riadiacich pobočiek by mali byť charakteristicky rovnaké, ale z možnosťou minimálnych odchýlení, ktoré sú spôsobené odlišnou lokalizáciou a požiadavkami klientov v daných geografických podmienkach. Uvedené odchýlenia sú charakterizované požiadavkami klientov a z hľadiska bezpečnosti sú ovplyvňované vývojom bezpečnostných incidentov ale aj vývojom kriminality za minulé obdobie.



Obr. 28. Definovanie jednotlivých pobočiek a ich funkcia v lokalizácií

ZDROJ: (autor)

Na uvedenom obrázku dochádza ku znázorneniu rozmiestnenia jednotlivých pobočiek a zároveň dochádza ku klasifikácii daného oddelenie. Riadenie organizácie je sústredené v meste Olomouc, pričom v danom objekte dochádza k najväčšiemu sústredeniu oddelení, a to primárne z vedenia jednotlivých poskytovaných služieb. Riadenie je sekundárne rozdelené na dva segmenty sústredené do Brna a Prahy. V uvedených riadiacich centrách dochádza ku vedeniu jednotlivých krajských miest s dôrazom na poskytované služby. Posledná úroveň pobočiek je charakterizovaná prostredníctvom monitorovacieho a servisného centra, kde dochádza ku základnému typu komunikácie s klientom a poskytovanie služieb.

3.3 Stavebné dispozície spoločnosti

Súčasná stavebná dispozícia jednotlivých kancelárskych priestorov nie sú konkrétne definované a nedochádza ku dokumentácii rozdelenia jednotlivých priestorov podľa oddelení. Jedná sa o absenciu uvedeného zasadacieho poriadku, ktorý by definoval, aké pracovné pozície a osoby ich zastupujúce sú sústredené v jednotlivých miestnostiach. Projektové plány by mali obecné definovať štruktúru jednotlivých pobočiek a kancelárskych priestorov, aby mohlo dochádzať k určovaniu možných rizík, ktoré v danom objekte môžu nastať. Jednou zo základných požiadaviek je teda práve určenie stavebných dispozícií s definovaním rozdelenia jednotlivých osôb na pobočke podľa najvhodnejšieho riešenia, ale jedná sa taktiež o logistické určenie dôležitých miestností.

3.4 Personálne zaistenie jednotlivých funkcií

Uvedená časť práce sa zaoberá popisom súčasného stavu personálneho zabezpečenia jednotlivých funkcií organizácie na jednotlivých pracoviskách. Dochádza k vymedzeniu funkcie uvedeného pracovníka a súčasnej dokumentácií súvisiacej s personálnym zabezpečením. V analytickej časti práce dôjde ku analýze uvedených informácií a po prípade k návrhu na zlepšenie.

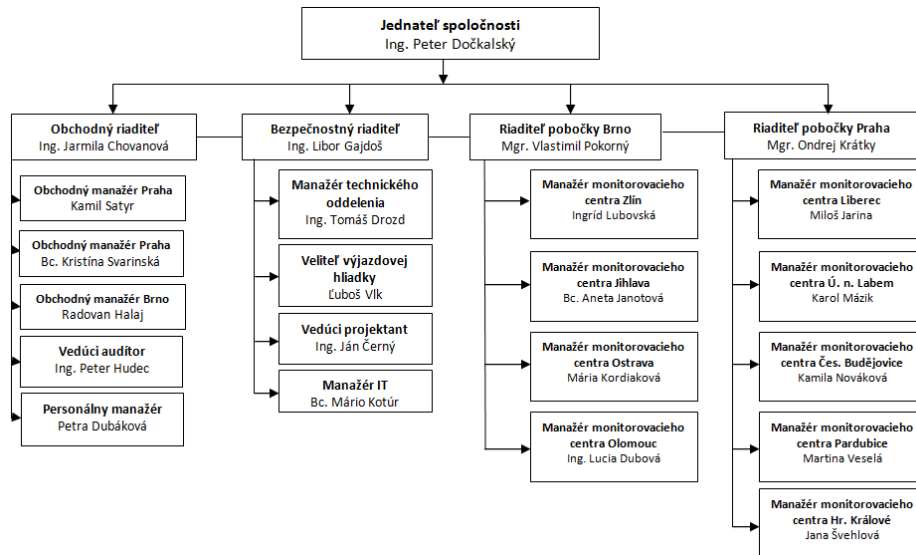
Tab. 5. Definovanie súčasného počtu zamestnancov na jednotlivých prevádzkach

Oddelenie	FUNKCIA	počet	Olomouc	Brno	Zlín	Jihlava	Ostrava	Praha	U. nad Labem	Liberec	České bud.	Pardubice	Hr. Kralove
Obchodné oddelenie	R obchodný riaditeľ	1	1										
	obchodný manažér	3		1				2					
	vedúci auditor	1	1										
	obchodný zástupca	27	2	3	3	2	3	3	3	2	2	2	2
	interný auditor	2	2										
Oddelenie bezpeč. manaž.	R bezpečnostný riaditeľ	1	1										
	veliteľ výjazdovej hliadky	1	1										
	manažér monitorovacieho centra	9	1		1	1	1		1	1	1	1	1
	riaditeľ pobočky	2		1				1					
	obsluha TPPC	54	4	8	4	4	4	10	4	4	4	4	4
	člen výjazdovej hliadky	85	6	12	6	6	6	20	6	6	6	5	6
	externý pracovník upratovacej služby	431	48	52	38	44	32	64	27	22	48	28	28
Personálne oddelenie	M externý pracovník strážny	375	33	65	44	36	21	87	18	12	18	23	18
	personálny manažér	1	1										
	personálny zástupca	5	2	1				2					
Technické oddelenie	M manažér technického oddelenia	1	1										
	M vedúci projektant	1	1										
	projektant	6	6										
	servisný technik	24	2	2	2	2	2	4	2	2	2	2	2
	bezpečnostný technik	10	6	2				2					
IT oddelenie	bezpečnostný konzultant	6	2	2				2					
	M manažér IT	1	1										
	IT technik	5	2	1				2					
Právnické oddelenie	fremný právnik	5	2	1			2						
Ekonomické oddelenie	ekonom	4	2	1			1						
spolu		686	128	152	98	95	69	202	61	49	81	65	61

ZDROJ: (autor)

Uvedená tabuľka definuje celkové počty zamestnancov na jednotlivých oddeleniach a zároveň ich zoskupuje do jednotlivých pobočiek, kde dochádza k výkonu práce. Zoradenie je podľa kompetencií smerom od vedenia k jednotlivým zamestnancom. Tabuľka definovania kompetencií definuje kompetencie na jednotlivých funkciách, kompetencie definujú procesy, ktoré jednotliví pracovníci vykonávajú. Dochádza len k čiastočnému určeniu kompetencií, pretože nie sú presne definované zodpovednosti. Návrhová tabuľka je uvedená v časti Prílohy pod názvom PRÍLOHA P IV.

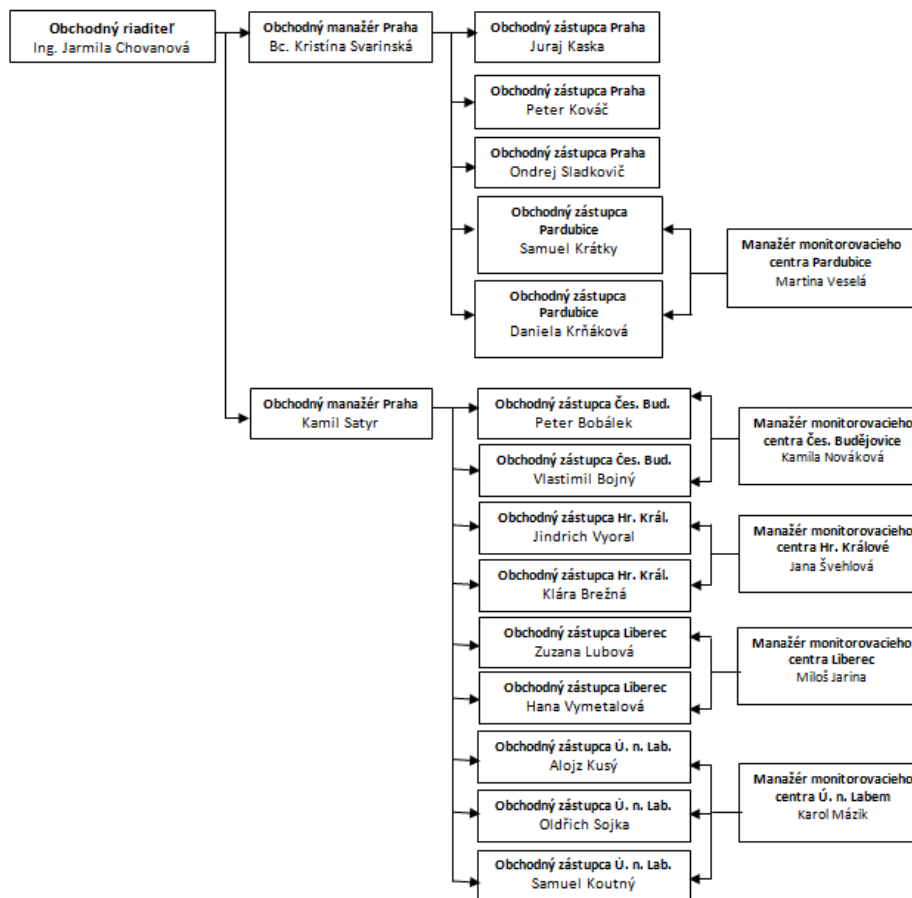
Kompetencie a zodpovednosti by mali byť definované do konkrétnych podrobností a malo by dochádzať k naviazanosti kompetencií na jednotlivé pracovné popisy, podľa vykonávanej práce. Uvedené určenie nebolo definované podľa popisu práce, ktorý by mal byť hodnotený v pravidelných intervaloch pre neustály proces zlepšovania zamestnancov.



Obr. 29. Definovanie spôsobu vedenia v organizácii

ZDROJ: (autor)

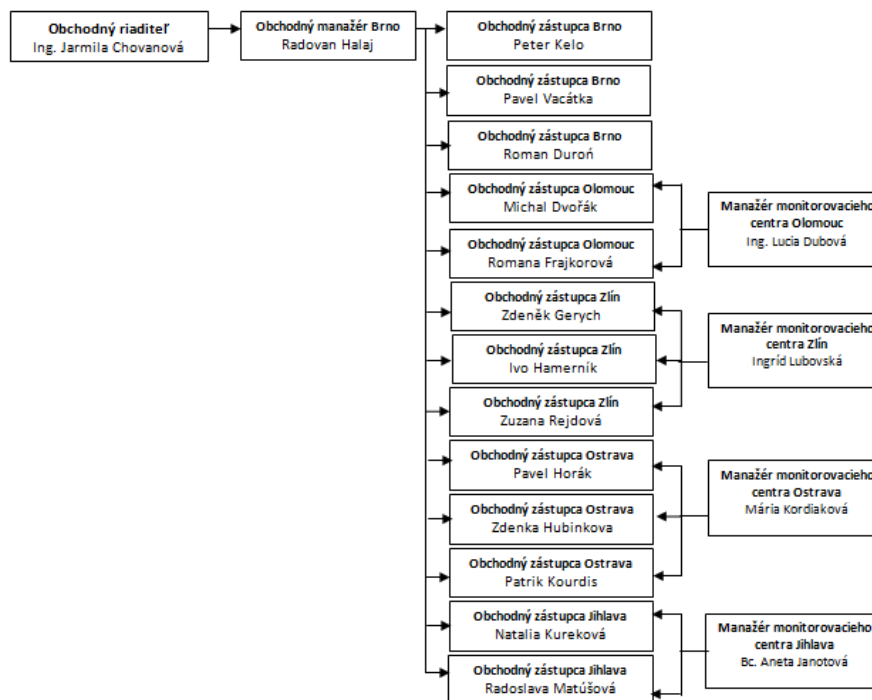
Nasledujúci obrázok zobrazuje usporiadanie obchodného oddelenia, pričom dochádza ku definovaniu konkrétnych osôb na daných pozíciách a zároveň dochádza k popisu lokality, v ktorej daná osoba vykonáva pracovnú pozíciu. Uvedené grafické znázornenie nám uľahčuje následné definovanie postupov, ale aj zamestnaneckých kariet, a to z dôvodu, že dochádza k prehľadnému definovaniu jednotlivých procesov ovplyvnenia výkonu povolania.



Obr. 30. Popis jednotlivých obchodných pozícií Praha

ZDROJ: (autor)

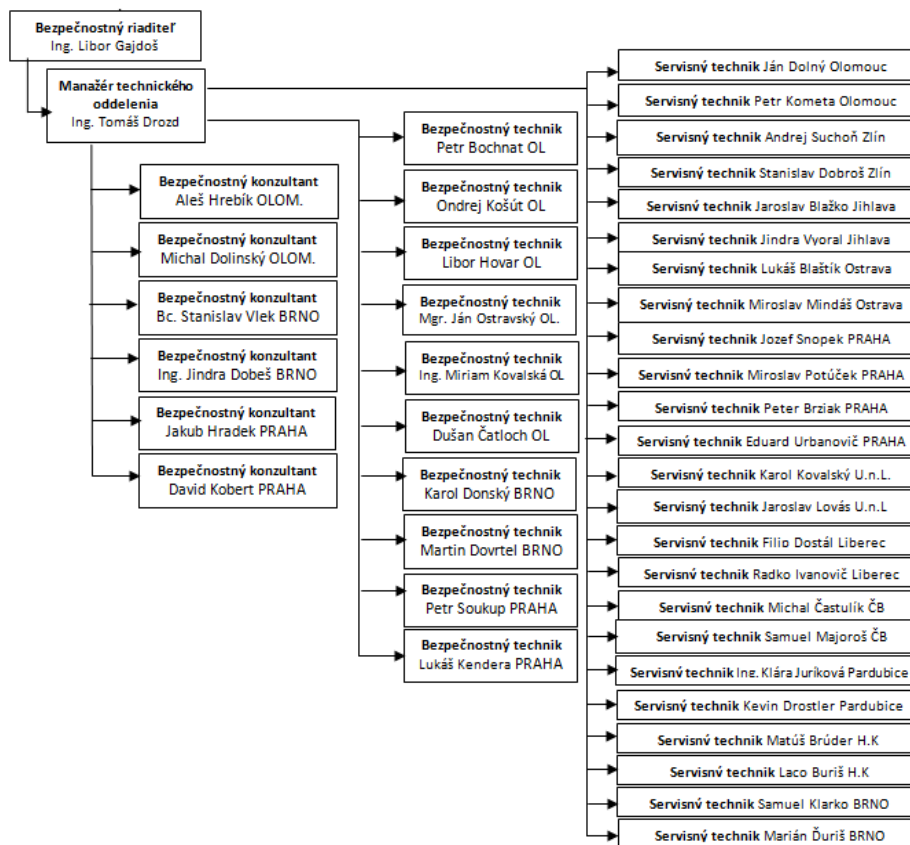
Ak dochádza ku vizualizácii stromu zodpovedností jednotlivých pozícií, dochádza u zamestnancov k uvedomeniu si primárneho vedenia nad ich funkciou, a teda dochádzame k názoru, že je nutné, aby konkrétny zamestnanci na pobočkách mali k dispozícii uvedený strom vedenia nad ich funkciou. Daný proces uľahčí riešenie problémov, ale aj ovplyvňovanie v prípade rozhodovania. Manažér monitorovacieho centra reprezentuje hlavnú vedúcu osobnosť na monitorovacom pracovisku, a súčasne by malo dochádzať k napĺňaniu dopredu určených a plánovaných procesov, ktoré by mali určiť vedúce osobnosti z daného oboru.



Obr. 31. Popis jednotlivých obchodných pozícií Brno

ZDROJ: (autor)

Oddelenie bezpečnostného manažmentu vedie bezpečnostný riaditeľ, ktorý zároveň vedie aj technické oddelenie organizácie. V sekundárnej línii vedie technické oddelenie technický manažér, ktorý vypracováva postupy pre bezpečnostných technikov, bezpečnostných konzultantov a servisných technikov a súčasne sa podieľa na plánovaní procesov v rámci vykonávania služby pre klientov. Technický manažér patrí do vedenia spoločnosti a zastupuje veľmi dôležitú úlohu, pretože definuje požiadavky, ako na zamestnancov, tak aj na ich výkon pracovnej činnosti. Jeho činnosť je primárne vykonávaná v sídle spoločnosti v Olomouci, ale keďže je v spoločnosti len jeden, jeho pracovná náplň zahŕňa cestovanie a plánovanie procesov po ostatných pobočkách v republike, za ktoré zodpovedá. V prípade konkrétnych pobočiek zastáva sekundárnu funkciu technického manažéra manažér monitorovacieho centra, ktorý riadi priamo chod danej pobočky a úzko spolupracuje s technickým manažérom. Je dôležité zdôrazniť potrebu neustáleho vzdelávania a rekvalifikácie technických zástupcov, a to či už na pozícií konzultanta, alebo technika. Každý technik by mal spĺňať dopredu definované zákonné, ale aj firemné požiadavky na výkon práce a jeho rekvalifikácie by mali byť trvalo zaznamenávané a kontrolované ich časové platnosti a intervaly.

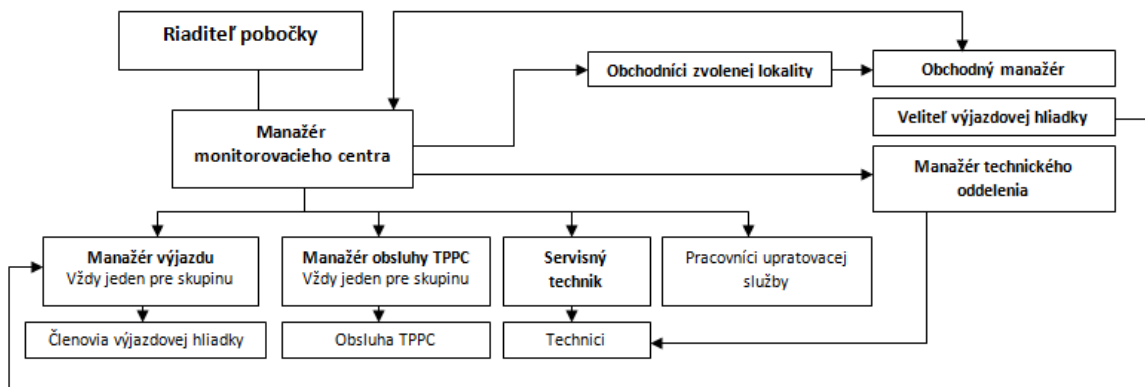


Obr. 32. Popis jednotlivých technických pozícií

ZDROJ: (autor)

Medzi jednu z ďalších vedúcich funkcií obchodného riaditeľa patrí vedenie ekonomického, právneho a auditorského tímu. Uvedené skupiny priamo vedie vedúci audítor, ktorý primárne a veľmi úzko spolupracuje s internými audítormi a na sekundárnej úrovni spolupracuje s právnym a ekonomickým oddelením. V súčasnej dobe nedochádza k definovaniu zodpovednej osoby priamo za ekonomické a právne oddelenie. Každý z uvedených zamestnancov v svojej štruktúre patrí primárne pod manažéra, alebo riaditeľa pobočky a súčasne pod definovaného priameho nadriadeného, ktorý v uvedenom prípade je vedúci audítor. Vedúci audítor zabezpečuje spoluprácu medzi právnikmi a ekonómami navzájom, a súčasne medzi požiadavkami ostatných oddelení, ktoré definujú požiadavky na dané osoby. Audítorsky tím je momentálne vo fáze budovania a prípravy spoločnosti na zlepšovanie svojich interných, ale aj externých procesov.

Nasledujúci obrázok definuje diagram činností, ktoré vykonáva manažér monitorovacieho centra, ktorý riadi chod pobočky, a to na úrovni obchodných vzťahov, vedenia tiesňového poplachového prijímacieho centra, a teda obsluhy, ale aj členov výjazdovej hliadky a zároveň servisných technikov a manažuje aj prácu pracovníkov upratovacej služby. Na sekundárnej úrovni sa daný manažér musí neustále radiť s vedením daných oddelení a vykonávať všeobecne platné predpisy pre dané odvetvie, ktoré by mali byť definované na rovnakej úrovni pre každú pobočku.



Obr. 35. Znáozornenie vedenia zo strany manažéra monitorovacieho centra

ZDROJ: (autor)

Z uvedeného diagramu činností všeobecne vyplýva, že osoba zastupujúca pozíciu manažéra monitorovacieho centra musí byť všestranné nadaná a vzdelaná, musí podliehať stresovej záťaž a súčasne vedieť správne riešenia veľmi zložitých situácií.

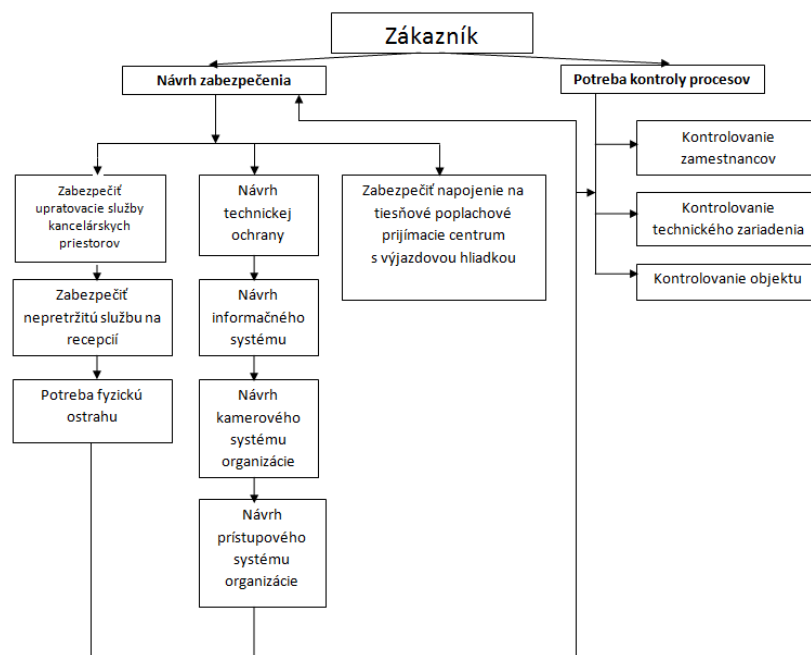
3.5 Ciele a funkcie podniku

V súčasnej dobe organizácia má za cieľ vytvoriť jednotný dokument reprezentujúci funkcie podniku s cieľom vytvárať pravidelné audity, a tým dosiahnuť získanie medzinárodných štandardov pre manažment riadenia kvality. Z uvedeného faktu je zrejmé, že je nutné spresniť požiadavky, ale aj celú politiku danej organizácie. Definovaním súčasných procesov, na ktorých je postavená činnosť organizácie dôjde k vykresleniu súčasnej situácie a zároveň k lepšiemu odhaleniu príležitostí na vznik hrozby.

3.5.1 Potreby potenciálneho zákazníka

Nasledujúci obrázok definuje potreby potenciálneho zákazníka vzhľadom ku službám, ktoré organizácia ponúka. Prioritne je nutné si uvedomiť nutnosť byť silne bezpečnou organizáciou vzhľadom k skutočnosti, že organizácia pracuje v sfére komerčnej bezpečnosti, a teda dochádza ku práci s dôvernými údajmi hlavne v sfére klienta. Ak chceme, aby klient vložil jeho bezpečnosť do našich rúk, musí samotná organizácia minimalizovať riziko napadnutia, čím by mohlo dôjsť k napadnutiu organizácie, ktorá reprezentuje zákazníka.

Zobrazenie vzťahu zákazníka a organizácie je primárne na dvoch úrovniach, kedy sa jedná o potrebu samotného návrhu zabezpečenia a kontrolu súčasného bezpečného systému a navrhnutie zmeny, alebo aktualizácie stavu vzhľadom ku hrozbám zákazníka.



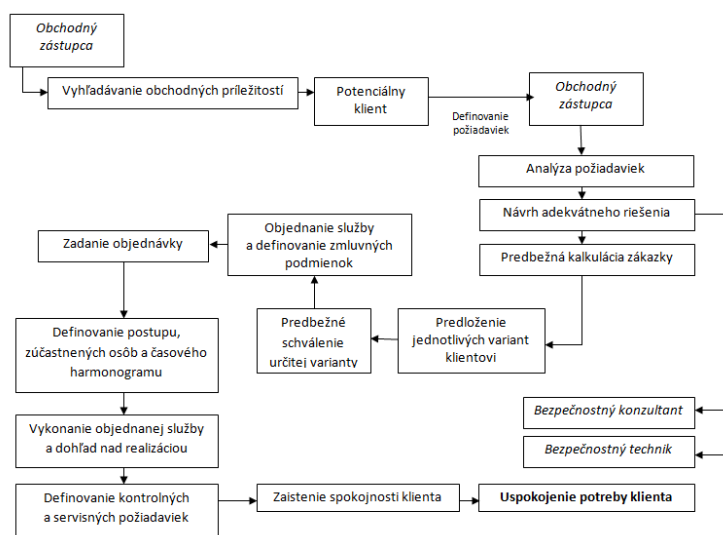
Obr. 36. Definovanie potrieb zákazníka vzhľadom ku organizácií

ZDROJ: (autor)

V procese poskytnutia služieb je najdôležitejším subjektom zákazník a pochopenie jeho potrieb, ktoré daný zákazník potrebuje uspokojiť v danom sektore. Ak budeme pri definovaní potenciálneho klienta rozmýšľať, ako potenciálny klient, je veľmi pravdepodobné, že veľmi blízko reálnosti definujeme skutočné potreby.

3.5.2 Definovanie procesu získania zákazky

Definovanie vzťahu funkcií organizácie po zadaní objednávky od zákazníka je vizualizované na nasledujúcom obrázku. V prvej úrovni dochádza ku vyhľadávaniu obchodných príležitostí obchodníkom. Uvedený proces je orientovaný na získanie potenciálneho klienta. V druhej fáze dôjde ku definovaniu požiadaviek klienta, ktorý má záujem o určité poskytnutie služieb, ktoré obchodný zástupca analyzuje spolu s bezpečnostným konzultantom a technikom navrhnu riešenie a dochádza k naceneniu uvedenej služby pre zákazníka, a to súčasne najvhodnejším riešením poskytovaním na trhu. Sekundárny proces začína schvaľovacím procesom klienta, kedy dôjde k spísaniu objednávky a definovaniu zmluvných podmienok, medzi ktoré patrí určenie predbežných termínov. V internom procese dochádza ku stanoveniu postupov a definovaniu časového rámca realizácie uvedenej zákazky.



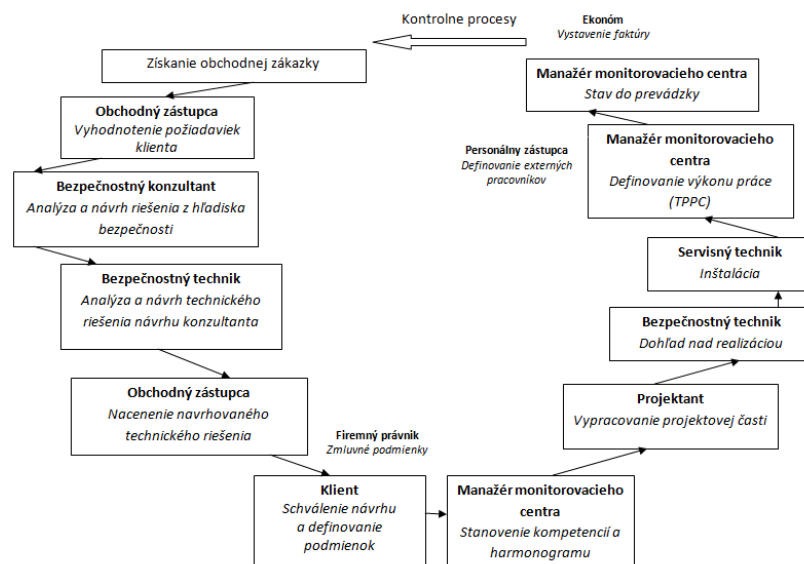
Obr. 37. Definovanie procesu objednávky služby zákazníka

ZDROJ: (autor)

Zákazka vo väčšine prípadov nekončí uvedením systému do prevádzky, ale následným kontrolovaním v čase, kedy dochádza k opakovaniu procesu nákupu zo strany zákazníka. Cieľom uvedeného procesu je uspokojenie potreby klienta, ktorá bola definovaná obchodným zástupcom na vstupe do obchodného vzťahu.

3.5.3 Definovanie procesu tvorby projektu

Uvedená časť práce popisuje rozdelenie funkcií pri tvorbe a realizácii produktu, ktorý si klient objednal. Jednotlivé funkcie sú definované vykonaním určitou osobou a funkciou v organizácii. Dochádza k zobrazeniu opakovaného procesu, kedy sa po určitej dobe od realizácie prvého produktu opakuje proces objednávky, ale je nutné poznamenať, že musí dochádzať ku zaujatiu klienta v prvom procese a vyvolaniu pocitu uspokojenia po dokončení diela u klienta. Ako ďalší veľmi dôležitý krok, je definovať služby tak, aby do budúcnosti bolo potrebné ich prehodnotenie, alebo aby dochádzalo k vyvolaniu potreby nutnosti realizovať inú službu.



Obr. 38. Diagram reprezentujúci pracovné činnosti na zákazke

ZDROJ: (autor)

V uvedenom procese chýba detekcia vstupu externej služby, ktorá v prípade potreby vykonáva čiastočnú funkciu. Je nutné si uvedomiť, že v prípade, že na klientove požiadavky využijeme poskytnutie služby externou firmou je nutné stanoviť podmienky dodania služby, ale aj proces reklamácie a dohľad nad realizáciou, a to z dôvodu, aby nedošlo ku poškodeniu mena firmy z dôvodu pochybenia zo strany externej firmy pri poskytovaní uvedenej služby.

Firma by mala uvedené procesy podrobovať pravidelnej kontrole, pričom by malo dochádzať ku strategickým zmenám na úrovni poskytovania služieb podľa požiadaviek klienta, pretože tak ako sa vyvíja prostredie, v ktorom žijeme, tak dochádza k vývoju

požiadaviek potenciálnych klientov, pretože tento vzťah na seba úzko súvisí. V dnešnej dobe rýchlych zmien nie je možné nevyvíjať metódy v organizácií za účelom neustáleho zlepšovania sa, a tým dosiahnutie trvalého udržania sa na trhu za cieľom zisku a prosperity celej organizácie.

4 ANALÝZA SÚČASTNÉHO STAVU

Nasledujúca časť práce sa zaoberá analýzou, ktorá vedie k procesu riadenia rizika, a to pomocou riadenia vyhodnotených rizík a plnením definovaných požiadaviek. Analýzu je nutné chápať ako proces, ktorý sa skladá z jednotlivých analytických metód, ktorými dochádzame k uvedomeniu si faktorov, ktoré ovplyvňujú vznik hrozby, ktorý sa vzťahuje k analyzovanému subjektu. Jednotlivé faktory nemusia byť len negatívne, ale aj pozitívne, ich odhalenie spôsobí, že následne môžeme uvedené faktory umelo vyvolať, alebo plánovať ich implementáciu za účelom zníženia negatívneho ohrozenia, alebo likvidáciu určitej hrozby. Dochádza k štylizácii odpovedí na primárne definovanie rizík, ktoré v organizácii hrozia, definovaniu pravdepodobnosti ich výskytu a následný odhad následkov, ktoré dané hrozby v prípade vyvolania bezpečnostného incidentu spôsobia. Analýza zohráva veľkú úlohu práve v stanovení bezpečnostných pravidiel organizácie.

4.1 Bezpečnostné posúdenie

Bezpečnostné posúdenie organizácie vedie ku zodpovedaniu základných otázok analytického procesu. Posúdenie je určené na kvalifikáciu základných nedostatkov, ktoré sú primárne viditeľné analytikom, ktorý daný problém rieši. Dochádza k formulácii cieľov, na ktoré je potrebné sa zamerať, pri odstraňovaní rizika.

Pre uvedenú realizáciu posúdenia došlo k využitiu tabuľkového hodnotenia. Nasledujúca tabuľka definuje primárne potreby organizácie a zároveň dochádza ku syntéze informácií a stanovení požiadavky, ktorá musí byť definovaná, aby mohlo dochádzať k určení procesov na zníženie možnosti vzniku incidentu v danom odvetví. Pri uvedenej tabuľke nedochádza ku hodnoteniu, ale dochádza iba k všeobecnému procesu zberu a validácie informácií.

Posúdenie bolo vyhotovené na základe informácií o cieľoch organizácie a ich súčasného stavu, v ktorom sa organizácia nachádza. Nedochádza k hodnoteniu, či uvedená organizácia má daný požadovaný prvok splnený. K hodnoteniu uvedených prvok dochádza v nasledujúcej časti práce, a to prostredníctvom použitia jednotlivých metód.

Definovanie cieľov organizácie				Určenie požiadavky
Technická ochrana objektov	vonkajšia ochrana objektu	zabezpečenie priestorovej ochrany	ochrana príjazdových ciest	určenie príjazdových ciest
			ochrana perimetru (optenie)	určenie rozlohy organizácie
			ochrana blízkeho okolia budovy	
		zabezpečenie plášťovej ochrany	zabezpečenie vstupných jednotiek (dvere)	definovať vstupné priestory
			zabezpečenie presklenných otvorov (okná)	
		vnútorná ochrana objektu	zabezpečenie elektronickej požiarnej signalizácie	zabezpečenie pred požiarom
	zabezpečenie poplachovým zabezpečovacím a tiesňovým systémom		zabezpečenie pred útočníkom	
	zabezpečenie prístupového systému		zabezpečenie proti neoprávnenému vstupu	
	Ochrana procesov v organizácii	ochrana interných procesov medzi zamestnancami	ochrana komunikácie	ochrana komunikácie pomocou technológií
ochrana manipulácie s projektovou dokumentáciou			ochrana osobnej komunikácie	
			ochrana pred neoprávneným zásahom neoprávnenej osoby	
ochrana pred neoprávneným rozosielaním				
ochrana pred nevedomosťou		definovať potrebné školenie a vzdelávanie		
ochrana externých procesov medzi zamestnancami a vonkajším prostredím		ochrana údajov spojených z chodom organizácie	definovať typ informácií a zaradenie	
		ochrana údajov spojených s klientom	definovať prácu s údajmi o klientovi	
	ochrana údajov spojených so súčasným dňom v organizácii	definovať typ informácií a zaradenie		
Ochrana života a zdravia v organizácii	ochrana života pri práci	ochrana pred smrťou	definovať nehody a skoro nehody	
		ochrana pred zranením	definovať percento pravdepodobnosti výskytu	
	ochrana zdravia pri práci	ochrana pred chorobou	definovať percento nehody a skoro nehody	
Zaistenie základných právnych predpisov	zaistenie plnenia právnych požiadaviek	zaistenie plnenia zákonov a právnych predpisov	definovanie podmienok	
		zaistenie plnenia platných právnych a technických noriem	definovanie podmienok	
	zaistenie, alebo príprava na plnenie noriem systému kvality	zaistenie podkladov definujúcich požiadavky pre danú certifikáciu	definovanie podmienok	
Zaistenie personálnej bezpečnosti	zaistenie plnenia definovaných požiadaviek na zamestnanca	zaistenie plnenia požiadaviek na zamestnaneckú pozíciu (vzdelanie, prax)	definovať požiadavky na pracovné pozície	
		zaistenie plnenia školiaceho procesu	definovať potrebné školenie a vzdelávanie	
Zaistenie spokojnosti klienta	zaistenie uspokojenia potreby klienta	zaistenie poskytnutia požadovaných služieb	definovať proces jednania z klientom	

Obr. 39. Definovanie primárnych cieľov bezpečnostnej politiky

ZDROJ: (autor)

4.1.1 Analýza pomocou SWOT analýzy

V nasledujúcej časti práce dochádza ku analytickému hodnoteniu pomocou aplikácie SWOT analýzy. Uvedená analytická činnosť je aplikovaná smerom od všeobecného ku konkrétnemu, pričom dochádza ku zameriavaniu sa na jednotlivé sektory, ktoré definujú čiastkové pod problémy, alebo faktory ovplyvňujúce problém.

4.1.1.1 Všeobecná aplikácia SWOT analýzy

Všeobecná aplikácia SWOT analýzy je zameraná na zistenie hodnoty jednotlivých silných a slabých stránok spoločnosti. Aspekt je určený váhou a hodnotou danej váhy, čo vyjadruje celkovú dôležitosť jednotlivých atribútov, alebo vlastností daného aspektu.

Tab. 6. Všeobecná aplikácia SWOT analýzy do podniku

SWOT analýza spoločnosť SECURITY consulting										
	pomocné					škodlivé				
	silné stránky	váha	hodnotenie		vyjadrenie v	slabé stránky	váha	hodnotenie		vyjadrenie v
vnútorne atribúty	definované produkty	0,01	4	0,04	4,0%	nedostatočné určenie pracovných náplní a kompetencií	0,013	-3	-0,039	3,9%
	orientácia na zákazníka	0,068	5	0,34	34,0%	nedostatočné strategické plánovanie	0,043	-3	-0,129	12,9%
	uvedomovanie si potreby bezpečnostnej politiky	0,095	4	0,38	38,0%	nedostatočné vedenie na nižšej úrovni	0,013	-1	-0,013	1,3%
	vytvorenie auditorského tímu	0,022	3	0,066	6,6%	nedostatočné definovanie postihov v prípade neplnenia požiadaviek	0,011	-2	-0,022	2,2%
	definovanie spôsobu vedenia	0,014	2	0,028	2,8%	nedostatočné školenia zamestnancov	0,087	-3	-0,261	26,1%
	definovanie oddelení	0,009	2	0,018	1,8%	absencia prístupového systému	0,079	-3	-0,237	23,7%
	vytvorenie IT oddelenia	0,005	1	0,005	0,5%	absencia informačného systému	0,081	-4	-0,324	32,4%
vonkajšie atribúty	príležitosti	váha	hodnotenie			hrozby	váha	hodnotenie		
	využitie zabezpečovacej techniky na zabezpečenie objektov organizácie	0,075	5	0,375	37,5%	ohrozenie konkurenciou	0,021	-2	-0,042	4,2%
	využitie poskytnutia služieb v oblasti IT	0,009	2	0,018	1,8%	neplnenie zákonných podmienok	0,1	-3	-0,3	30,0%
	vytvorenie systému spätnej väzby od zákazníka	0,019	3	0,057	5,7%	zniženie úrovne kvality služieb v časovom vývoji	0,046	-4	-0,184	18,4%
	vytvorenie presných podmienok pre dodávateľov služieb	0,017	4	0,068	6,8%	ohrozenie útokom cudzej osoby na organizáciu	0,045	-5	-0,225	22,5%
	zvýšiť bezpečnosť pri vykonávaní práce mimo objekty organizácie	0,087	4	0,348	34,8%	ohrozenie útokom na informačný systém	0,032	-5	-0,16	16,0%
spolu váha							100%			

ZDROJ: (autor)

Uvedená analýza je spracovaná pomocou určenia váhy v intervale od 1 do 5, pričom hodnota 1 vyjadruje najnižšiu spokojnosť a hodnota 5 vyjadruje najvyššiu spokojnosť. V prípade hodnotenia škodlivých atribútov a hrozieb je hodnotenie v intervale od -1 do -5. Hodnotou -1 je definovaná najnižšia nespokojnosť a hodnota -5 definuje najvyššiu

nespokojnosť. Váha bola stanovená pomocou vyjadrenia dôležitosti jednotlivých atribútov pre subjekt. Konkrétne určenie bolo predmetom konzultácií s riadením organizácie, a to prostredníctvom vyjadrenia dôležitosti pre naplnenie cieľov organizácie.

Nasledujúce hodnotenie vyjadruje jednotlivé vynásobenie hodnoty váhy a číselnej hodnoty atribútu, ktoré je následne spočítané a vyhodnotené na internej a externej úrovni. Pre získanie celkového hodnotenia dochádza k súčtu hodnotenia vnútorných a vonkajších atribútov.

Tab. 7. Bilancia súčasného stavu organizácie

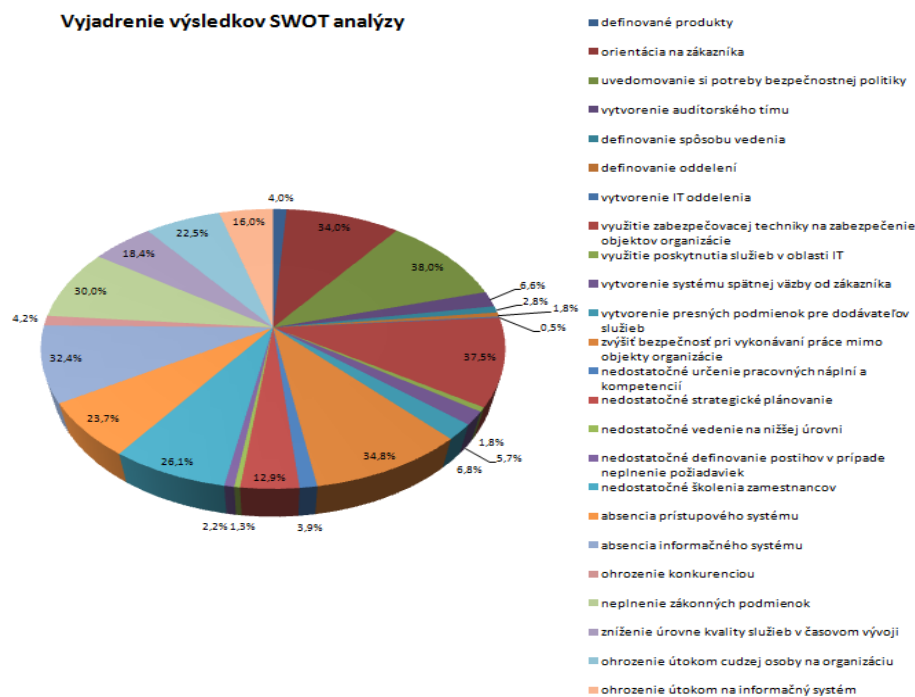
CELKOVÉ HODNOTENIE	-0,193		
vnútorné atribúty	0,877	-1,025	-0,148
vonkajšie atribúty	0,866	-0,911	-0,045

ZDROJ: (autor)

Súčasný stav organizácie nie je príliš lichotivý, a ako je možné vidieť v uvedenej hodnotiacej tabuľke, v zápornejších hodnotách sa pohybujú vnútorné atribúty na ktorých je nutné zapracovať. Pri hodnotení dochádza k vyjadreniu v percentuálnej hodnote, a to z dôvodu, že dochádza ku zreteľnejšiemu pohľadu na závažnosť jednotlivých problémov. Jedná sa o primárnu analýzu, ktorá v ďalších krokoch podlieha opätovnému hodnoteniu.

Navrhovaná tabuľka je vytvorená tak, aby uvedený nástroj riadenia mohol byť použitý pre opätovné hodnotenie, a teda aj pri zmene jednotlivých reprezentujúcich údajov dochádza k veľmi rýchlemu vyhodnoteniu a možnému zobrazeniu súčasnej situácie. Pri hodnotení je veľmi efektívne uvedomiť si zápornú hodnotu a jednotlivé metódy hodnotenia, ale aj stanoviť interval hodnôt.

Graf 1. Grafické vyjadrenie percentuálnych výsledkov SWOT analýzy



ZDROJ: (autor)

Grafické vyjadrenie hodnotenia nepracuje zo zápornými hodnotami, ale dochádza ku porovnaniu a vizualizácii jednotlivých percentuálnych hodnôt, ktoré danú analýzu reprezentujú. Uvedené vyjadrenie je orientačné a slúži pre porovnanie dôležitosti jednotlivých atribútov, ktoré spoločne pôsobia na chod organizácie.

4.1.2 Analýza pomocou úvodnej analýzy nebezpečenstva

Uvedený druh analýzy je použitý pre analýzu určitého sektoru organizácie. V úvode dochádza ku použitiu uvedenej metódy na definovanie možnosti zranení a následkov. Uvedený druh metódy je možné použiť aj pre pod analýzu, ktorej prechádzala analýza, ktorá vyhodnotila určité odvetvie, ako nedostatočne zabezpečené proti hrozbám. Dochádza k definovaniu početnosti výskytu určitej hrozby, vzhľadom na stupeň poškodenia, ktorý hrozí v prípade, že daná hrozba nastane v časovom intervale súčasnosti.

V prípade hodnotenia nehody, alebo rizika vzniku nehody je veľmi dôležité registrovať aj nehody, ktoré v minulosti ešte nenastali, ale došlo k podmienkam, kedy daný druh nehody bezprostredne hrozil, a v prípade, že by nedošlo k aplikácii určitých pravidiel, skoro nehoda by bola definovaná, ako nehoda. V praktickom využití je nutné si následne uvedomiť aj aspekty, ktoré vytvorili v danej situácii prostredie, v ktorom nedošlo k nehode a následne

definovať situácie, v ktorých daný postup môžeme, alebo musíme aplikovať, a tým znížime riziko vzniku danej situácie.

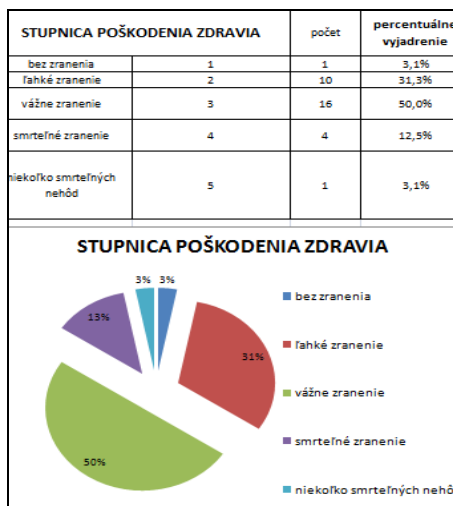
Tab. 8. Úvodná analýza hrozby zranenia

ÚVODNÁ ANALÝZA NEBEZPEČENSTVA ZRANENIA	Definovanie druhu nehody	Definovanie pracovnej činnosti	počet skoro nehôd za 1 rok	počet nehôd za 1 rok	početnosť	stupeň možného poškodenia zdravia	INDEX RIZIKA
		ľahké zranenie končatiny (odreniny, modřiny)	pádóm pri montáži	nutné registrovať aj skoro nehody	48	9	1
	pomliaždenia končatiny	pádóm pri montáži	5		2	7	
	zlomenina končatiny - ľahká	pádóm pri montáži	2		9	2	11
	viacnásobná zlomenina končatiny	pádóm pri montáži	5		3	8	
	otvorená zlomenina končatiny	pádóm pri montáži	4		2	6	
	otras mozgu - ľahký	pádóm pri montáži	4		9	2	11
	otras mozgu - ťažší	pádóm pri montáži	1		9	3	12
	strata vedomia	pádóm pri montáži	5		3	8	
	otvorená rana - ľahká (spôsobená cudzím predmetom)	pádóm pri montáži	4		2	6	
	otvorená rana - ťažká (spôsobená cudzím predmetom)	pádóm pri montáži	4		3	7	
	zasiahnutie elektrickým prúdom	inštalácia a servis	1		9	3	12
	ľahké zasiahnutie elektrickým prúdom	inštalácia a servis	4		4	4	8
	zranenie oka bez následkov		2		2	4	
	zranenie oka s následkami		2		3	5	
	zranenie tváre ľahké		2		2	4	
	Zlomenina lebečnej kosti	pádóm pri montáži	2		3	5	
	ľahké poškodenie chrbtice	pádóm pri montáži	4		2	6	
	poškodenie miechy	pádóm pri montáži	4		3	7	
	zlomenina chrbtice	pádóm pri montáži	4		4	8	
	zlomenina panvy	pádóm pri montáži	4		3	7	
	úrazy brucha	pádóm pri montáži	5		3	8	
	roztrhnutie orgánu v dutine brušnej v dôsledku úrazu	pádóm pri montáži	3		3	6	
	poškodenie pľúc	pádóm pri montáži	4		3	7	
	poškodenie srdca	pádóm pri montáži	4		3	7	
	poranenia nervovej sústavy ľahké	zasiahnutím elektrickým prúdom	3		2	5	
	poranenia nervovej sústavy ťažké	inštalácia a servis	3		3	6	
	inštalácia a servis						
	poleptanie a popálenie pokožky do 10cm		2		2	4	
	poleptanie a popálenie viac do 10% tela		2		3	5	
	poleptanie a popálenie do 50%		2		4	6	
	poleptanie alebo popálenie viac ako 50% tela		2		5	7	
	vnútorné krvácanie	pádóm pri montáži	5		3	8	
	zástava srdca	pádóm pri montáži	5	4	9		

ZDROJ: (autor)

Uvedený druh analytického nástroja je definovaná spôsobom, aby dochádzalo ku automatickému prepočtu jednotlivých údajov, ale aj k prepočtu indexu rizikovosti, ktorý je vyjadrený súčtom početnosti a stupňa možného poškodenia. Uvedené vyjadrenia definujú nasledujúce obrázky.

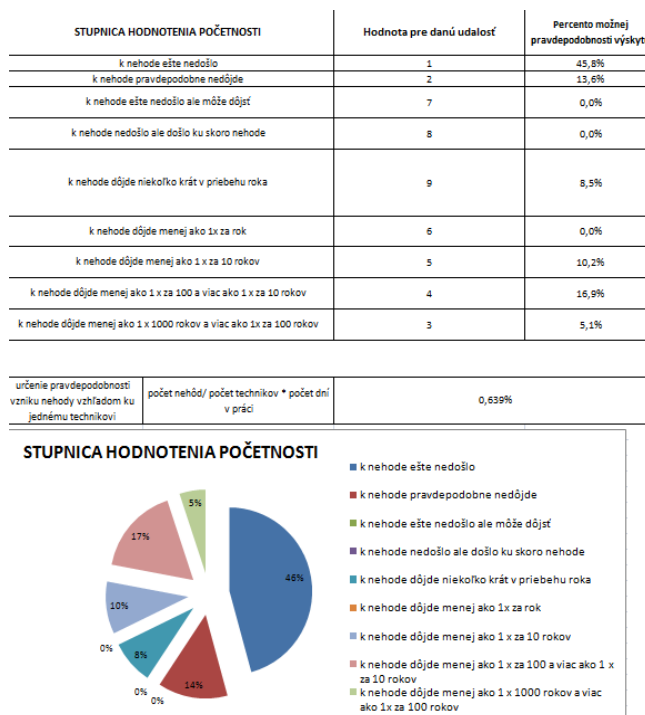
Stupnica poškodenia zdravia je definovaná hodnotami v intervale od 1 do 5, pričom číselná hodnota 1 vyjadruje najmenej vážne zranenie, alebo poškodenia zdravia a hodnota 5 vyjadruje najväčšie zranenie alebo poškodenie zdravia. Následné percentuálne vyjadrenie hodnôt početnosť daného poškodenia vzhľadom ku všetkým definovaným poškodeniam, teda dochádzame ku štatistickému záveru, akých zranení a poškodení dochádza najviac v danej organizácii.



Obr. 40. Definovanie vyhodnoteného vzťahu stupnice zranení a ich počet

ZDROJ: (autor)

Uvedený obrázok definuje vzťahy vyplývajúce z jednotlivých metód hodnotenia a k percentuálnemu vyjadreniu závislosti jednotlivých typov zranení na ich početnosti a na stupnici poškodenia jednotlivých úrazov. Je zrejmé, že v súčasnom stave bolo dokumentovaných až 50 % zranení zo všetkých dokumentovaných zranení, ktoré boli charakterizované, ako vážne.



Obr. 41 Definovanie vyhodnotenia stupnice hodnotenia početnosti zranení

ZDROJ: (autor)

Uvedené vyjadrenie hodnotenia početnosti zranenia je v prvotnej fáze realizované určením hodnoty pre danú časovú frekvenciu výskytu udalosti. Následne dochádza k hodnoteniu koľko krát sa v uvedenom analytickom procese vyskytol určitý druh hodnotiaceho atribútu, s čoho je následne určený percentuálny údaj vyjadrujúci časový výskyt jednotlivých definovaných zranení.

4.1.3 Analýza vplyvom porúch a následkov v procese organizácie

Analýza vplyvom porúch a následkov je v prípade uvedenej organizácie aplikovaná na hodnotenie nedostatkov v procese primárneho cieľa organizácie. Základné pravidlo odpovedá na otázky týkajúce sa konkrétneho procesu, ktorý môže byť poškodený. Následne dochádza k otázke, kde dochádza k vzniku chyby, teda dotýka sa daný problém konkrétneho oddelenia podniku. Na záver dochádza ku definovaniu závažnosti, pričom dochádza k pravdepodobnostnému určeniu dôsledkov, ktoré môžu nastať.

V procese analýzy dochádza k primárnemu zodpovedaniu nasledujúcich otázok:

- **Čo môže poškodiť proces?** – Dochádza k sekundárnemu deleniu na všeobecný typ poškodenia a na konkrétnu udalosť, ktorá je v uvedenej kategórii.
- **Kde môže dôjsť k poškodeniu procesu?** – Daná otázka definuje možné pod procesy, ktorých nespĺnením, alebo ich nedostatočným plnením môže dôjsť ku vzniku poškodenia alebo poruchy, pričom v sekundárnej fáze dochádza ku konkrétnemu definovaniu oddelenia, na ktorom dochádza ku poškodeniu.
- **Aké závažné je poškodenie?** – Otázka špecifikuje samotný proces hodnotenia hroziaceho poškodenia. Uvádza sa kategória kritickosti, ktorá je následne v hodnotení definovaná číselnou hodnotou.

Tab. 9. Vyjadrenie vzťahu medzi kategóriou kritickosti a hodnotou

HODNOTENIE/ kategória kritickosti	
Katastrofická	4
Kritická	3
Okrajová	2
Zanedbateľná	1

ZDROJ: (autor)

V nasledujúcej tabuľke dochádza v procese určenia závažnosti aj k definovaniu možného dôsledku. Dôsledok pre uvedenú analýzu reprezentuje najvyššiu možnú situáciu, ktorá v dôsledku nesplnenia predchádzajúcich podmienok, môže nastať. Jedná sa ale aj o faktor časového pôsobenia, čo znamená, ako dlho dané požiadavky neboli splňované.

Tab. 10. Analýza vplyvom porúch a následkov v projekte

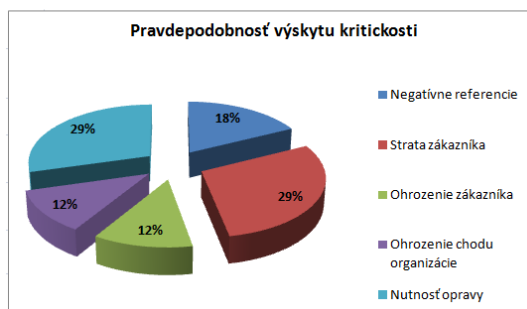
Analýza vplyvom porúch a následkov								
Čo môže poškodiť proces?		Kde môže dôjsť k poškodeniu procesu?				Aké závažné je poškodenie?		
Druh poruchy	Technické oddelenie	SERVIS	INŠTALÁCIA	Obchodné oddelenie	Katégoria kritickosti	Dôsledky	Hodnotenie	
Chyba v projekte	Chyba v analýze zákaznických potrieb	CHYBA v celom nasledujúcom procese			Nedostatočné školenie obchodných zástupcov	Neodstránenie chyby v počítačovej fáze Katastrofická	STRATA ZÁKAZNÍKA	4
	Chyba v návrhu komponentov	Nedostatočná kontrola správnosti	CHYBA v celom nasledujúcom procese		Nedostatočné vedomosti o technických komponentoch	Neodstránenie chyby v počítačovej fáze Katastrofická	STRATA ZÁKAZNÍKA Vytvorenie negatívnych referencií	4
Porucha na komponente	Nesprávna funkčnosť technického komponentu určeného k montáži		Reklamácia dodaného komponentu - CHYBA Z VÝROBY	SKONTROLOVANIE KOMPONENTOV - pred montážou	Nedostatočné zaistenie podmienok spolupráce pre dodávateľov	Nesplnenie časového plánu zákazníka jeho negatívne ovplyvnenie činnosti Kritická	STRATA ZÁKAZNÍKA Vytvorenie negatívnych referencií	3
	Nedodržanie postupu inštalácie komponentov a nesprávna funkčnosť celého systému	Chyba v určovaní procesu inštalácie vychádza sa z postupov od výrobcu a vzájomného ovplyvnenia		Nedodržanie určených postupov k inštalácii		Nedostatočná profesionalita vzhľadom k zákazníkovi Katastrofická	STRATA ZÁKAZNÍKA Vytvorenie negatívnych referencií	4
	Nedodržanie postupu inštalácie komponentov zo spôsobením poruchy na jednom komponente	Chyba v určovaní procesu inštalácie vychádza sa z postupov od výrobcu		Nedodržanie určených postupov a technických pravidiel k inštalácii		Nedostatočná profesionalita vzhľadom k zákazníkovi Kritická	Možná strata zákazníka Vytvorenie negatívnej skúsenosti	3
	Výskyt poruchy po určitej dobe - porucha v prenosovej ceste		Nutnosť klasifikovať vznik poruchy a odstrániť následky ale hlavne odstrániť príčinu vzniku poruchy	Nedostatočné predvídanie novej poruchy		Nedostatočná profesionalita vzhľadom k zákazníkovi Okrajová	Možný odchod zákazníka ku konkurencii Zmena z dôvodu poskytnutia lepších služieb	2
	Výskyt poruchy po určitej dobe - porucha v povelu systému		Nutnosť klasifikovať vznik poruchy a odstrániť následky ale hlavne odstrániť príčinu vzniku poruchy	Nedostatočné predvídanie novej poruchy - nutné klasifikovať zmeny v systéme		Nedostatočná profesionalita vzhľadom k zákazníkovi Okrajová	Možný odchod zákazníka ku konkurencii Zmena z dôvodu poskytnutia lepších služieb	2
Poškodenie systému	Poškodenie prístupového systému internou činnosťou organizácie	Nedostatočné určenie požiadaviek na obsluhu systému internými pracovníkmi	Pravidelné preškoľovanie organizácie a servisné kontroly			Negatívne ovplyvnenie chodu organizácie Okrajová	Nutnosť urgentne reagovať servisom Strata vzhľadom na zákaznickovú organizáciu	2
	Poškodenie informačného systému internou činnosťou organizácie	Presné definovanie funkcií a možnosti nastavení - definovať zázaky	Pravidelné preškoľovanie organizácie a servisné kontroly			Negatívne ovplyvnenie chodu organizácie - vznik interných problémov Okrajová	Nutné znovu investície do obnovy systému a dát Ohrozenie stability podniku	2
	Nedodržanie servisných opatrení		Definovanie plánov po servise			Možnosť vzniku poškodenia systému a obmedzenie organizácie Okrajová	Nutné znovu investície do obnovy systému a dát Ohrozenie stability podniku	2
	Poškodenie interného systému - zabezpečenie objektu	Určiť presné požiadavky na systém a definovať možné krízové stavy - SYSTÉM ORGANIZÁCIE MUSÍ BYŤ ČO NAJBLIŽŠIE IDEÁLNEMU	PRIORITNÝ SERVIS PRE FUNKCIU ZÁKAZNÍKOM	Zapojenie do systému krízových opatrení	Oznámenie zákazníkom OBMEDZENÝ STAV	V prípade zistenia chyby zákaznikov - strata zákaznikov - ZLE REFERENCIE Katastrofická	Nutné znovu investície do obnovy systému a dát Ohrozenie stability podniku	4
	Poškodenie interného systému - dochádzkový systém							4

ZDROJ: (autor)

Analýzou dochádzame k záverom, ktoré sú veľmi dôležité na určenie opatrení pre zníženie možnosti vzniku kritickej udalosti, ktorá má za následok dôsledky uvedené v hodnotení. Po uvedenom zložitom analytickom procese dochádza k hodnoteniu, ktoré je zobrazené formou percentuálneho vyjadrenia jednotlivých závažných dôsledkov. Závažné dôsledky, ktoré majú veľmi významný negatívny vplyv na primárny cieľ organizácie sú nasledujúce.

Uvedené analytické vyhodnotenie je výsledkom uvedenia vzájomného vzťahu medzi dôsledkom, ktorý je uvádzaný od najnižšej úrovne závažnosti danej skutočnosti až po najvyššiu úroveň, výskytom kategórie kritickosti, ktorá daný dôsledok spôsobuje a početnosťou, ktoré reprezentuje počet výskytu uvedeného incidentu v danej analýze. Pravdepodobnosť vyjadruje percentuálnu možnosť, že daný incident nastane a bude viesť až ku dosiahnutiu dôsledku.

Dôsledok	Kategória kritickosti	Početnosť výskytu	Pravdepodobnosť
Negatívne referencie	4	3	25%
Strata zákazníka	4	5	42%
Ohrozenie zákazníka	3	2	17%
Ohrozenie chodu organizácie	4	2	17%
Nutnosť opravy	2	5	42%



Obr. 42. Analýza vplyvom porúch a následkov

ZDROJ: (autor)

Z grafického znázornenia hodnotenia je viditeľné, že najrizikovejším dôsledkom, ale aj najväčším je strata zákazníka, ktorá môže viesť ku negatívnym referenciám, a tým k strate ďalších potenciálnych zákazníkov. V prípade, že dôjde ku zákazníkovej nespokojnosti je nutné zaznamenávať dôvody, ktoré viedli k jeho nespokojnosti a následne ich vyhodnotiť a určiť, či došlo k chybe v procese poskytovania služby, a ak áno, kde daná chyba vznikla. Uvedená analýza hodnotí proces obchodného vzťahu, ktorý vedie spoločnosť k zisku, a to je hlavný cieľ pre udržanie spoločnosti na trhu. Pre uvedený cieľ zisku je nutné eliminovať faktory, ktoré by v ďalšej fáze spôsobovali negatívne účinky, a to vo forme negatívnych referencií, ktoré by následne viedli k zníženiu účinnosti prostriedkov nasadených na získanie potenciálneho klienta. Je všeobecne známy fakt, že najlepšou reklamou je pozitívna referencia na daný subjekt.

Proces:		Získanie klienta			
vyhľadavanie možností pre získanie klienta	oslovenie potenciálneho klienta	získanie konkrétnych požiadaviek klienta	spokojnosť klienta	získania zákazky (zmluvy)	
↑	↑	↑			
definovanie potenciálnych klientov	útok na potrebu klienta	potreba uspokojíť klienta a poskytnúť mu vhodné riešenie v krátkom časovom intervale			

Obr. 43. Proces získania klienta

ZDROJ: (autor)

Na uvedenom obrázku dochádza k znázorneniu procesu získania klienta, ktorý vedie k získaniu zákazky a v prípade naplnenia požiadaviek dochádza k spokojnosti klienta, a teda k jeho opätovnému procesu nákupu a súčasne ku pozitívnej reklame vo forme referencií.

Proces:		Tvorba projektu			
DEFINOVANIE ZMLUVNÝCH PODMIENOK	SCHVÁLENIE A ZAHÁJENIE PROJEKTU			DODRŽIAVANIE ČASOVÝCH INTERVALOV	SANKCIE
Požiadavky klienta	Obhliadka objektu			Zahájenie činnosti	Definovať aké nám hrozia
	Vyjadrenie k poskytovanej službe			Dodávka materiálu	
Časový plán (potreba klienta)	<i>technické oddelenie</i>		<i>manažér monitorovacieho centra</i>	Inštalácia	Kontrolovať
	<i>určenie konkrétnych fáz</i>		<i>plánovanie kontrol</i>	Zaškolenie	
Plán jednotlivých fáz projektu	<i>časové plnenie</i>		<i>definovanie dohľadu</i>	Skúšobný režim	Upozorňovať
	<i>určenie zainteresovaných osôb</i>		<i>zainteresovanie do plánu obhliadok výjazdovej hliadke</i>	Servisné opatrenia	
Definovanie zmluvných pokút	<i>definovanie zodpovedností</i>		<i>definovanie upratovacích pracovníkov</i>	Zavedenie do stavu funkčnosti	Vymáhať
	<i>projektčné oddelenie</i>		<i>definovanie recepcných pracovníkov</i>	Pravidelný servis	
Definovanie rozsahu poskytnutia služby	<i>zahájenie projektového riadenia</i>		<i>definovanie iných bezpečnostných pracovníkov</i>	Vedenie záznamov o zmene	Vyrovnáť
	<i>vytvorenie projektu</i>			Vedenie záznamov o kontrole napĺňovania zmluvných podmienok	
	Definovanie kontroly				

Obr. 44. Proces tvorby projektu po získaní zákazky

ZDROJ: (autor)

Proces tvorby projektu je definovaný všeobecnými primárnymi prvkami, ktoré reprezentujú jednotlivé časti, ktoré by mali byť napĺňované. Dochádza k definovaniu nového atribútu a to vo forme uvedomovania si sankcií, s čoho vyplýva potreba definovať nesplnenie podmienok a upozorňovať na dané nezrovnalosti, a to či už na vymáhanie sankcií, ktoré nadobudli svoju účinnosť vzhľadom ku porušeniu podmienok uzavretých z organizáciou, alebo sankcie, ktoré hrozia, že budú vymáhané od klienta, a to vznikom nároku z nesplnenia zmluvných podmienok.

4.1.4 Analýza príčin a následkov

Uvedený typ analýzy bol využitý pre dva analytické procesy a to hodnotenie fyzického útoku na organizáciu a hodnotenie spoľahlivosti zamestnancov. Analýza spoľahlivosti zamestnancov úzko súvisí s analýzou spoľahlivosti človeka, ktorá je podrobnejším pokračovaním získaných informácií.

Tab. 11. Analýza fyzického útoku na objekt

Fyzický útok na objekt														
CIEĽ	získanie finančnej hotovosti		získanie materiálu (sklad)		poškodenie mena spoločnosti		vandalizmus		získanie informácií o spoločnosti		získanie informácií o klientoch a ich objektoch			
ÚTOČNÍK	útočník bez znalostí		útočník so základnými znalosťami		útočník veľmi skúsený		útočník bez znalostí		útočník veľmi skúsený		útočník veľmi skúsený			
VÝSKYT	13%		15%		17%		15%		21%		19%			
UDALOSTI	Dochádza v objekte k kumulácii peňazí?	4	Dochádza v objekte k voľnému pohybu cudzích ľudí?	3	Je spoločnosť verejne známa?	4	Dochádza v objekte k voľnému pohybu cudzích ľudí?	3	Je spoločnosť v procese, kde by mohlo dochádzať ku potrebe odhaliť utajované informácie?	4	Dochádza ku evidencii papierových projektov?	4		
	Dochádza v objekte ku predaju a nákupu?	3	Je verejne známe, že v objekte sa kumuluje materiál o vyššej finančnej hodnote?	4	Bojuje spoločnosť s vysokou mierou konkurencie?	4	Má spoločnosť verejných nepriateľov?	3	3,4	Disponuje spoločnosť s tajnými informáciami?	5	Sú klientové informácie rozdeľované podľa citlivosti?	3	
	Obsahuje objekt trezory?	2	2,5	Obsahuje sklad zabezpečenie proti vniknutiu?	4	2,83	Má spoločnosť verejných nepriateľov?	3	3	Má spoločnosť ochránené informačné technológie?	2	4	Je definovaný postup s informáciami o klientoch?	4
	Je objekt chránený mechanickými zbraňami systémami?	2		Je objekt chránený mechanickými zbraňami systémami?	2		Dochádza v spoločnosti ku externým nehodám?	3	3	Zdieľajú zamestnanci informácie v rámci firmy?	5			
	Je objekt chránený elektronickým zabezpečovacím systémom?	2		Je objekt chránený elektronickým zabezpečovacím systémom?	2		Má spoločnosť informačný systém?	3	3	Bol v minulosti objekt poškodený vandalizmom?	3			
	Je v objekte kamerový systém?	2		Je v objekte kamerový systém?	2					Dochádza ku kontrole práce na počítačoch? Hrozí nebezpečením?	4		Dochádza ku záznamu osôb ktoré manipulujú s dátami?	4
												3,75		

ZDROJ: (autor)

Hodnotenie analýzy fyzického útoku prebieha v dvoch procesoch. V úvode dochádza ku stanoveniu otázok, ktoré s danou problematikou úzko súvisia, pričom sa vychádza zo všeobecných cieľov útoku a vedomostí páchateľa. Nasledujúce hodnotenie primárne určí, či udalosťou, na ktorú bol vznesený dotaz dochádza ku ohrozeniu organizácie. Je nutné si uvedomiť, že hodnotenie nedefinuje pravdepodobnosť, či sa daná otázka vyskytuje v praktickom chode firmy.

Tab. 12. Hodnotenie analýzy príčin následkov

HODNOTENIE	
ÁNO hrozí	5
prevažne áno hrozí	4
skôr nie nehrozí	3
obsahuje niektoré bezpečnostné prvky	2
NIE nehrozí je zabezpečený	1

ZDROJ: (autor)

Uvedené hodnotenie definuje pri analýze jednotlivé číselné hodnoty. V odpovedaní na dotazy dochádza ku všeobecne pochopiteľnému vyjadreniu, či došlo k nasadeniu prostriedkov na minimalizovanie hrozby, ktorá hrozí uvedenou otázkou.

Tab. 13. Vyhodnotenie hrozby fyzického útoku na organizáciu

	Celková hodnota	Počet výskytu	Priemerná hodnota
Na hlavnú udalosť	19,48	6	3,25
Na jednotlivé udalosti	93	29	3,21

ZDROJ: (autor)

Vyhodnotenie hrozby vzniku udalosti spojenej s fyzickým útokom na organizáciu definuje priemernú hodnotu vzniku krízovej udalosti v danom segmente analytického procesu. Na jednotlivú udalosť pripadá hodnota 3,21, ktorá je definovaná ako udalosti, ktoré primárne nehrozia, a teda sú v určitej miere chránené.

Tab. 14. Analýza spoľahlivosti zamestnancov

Analýza spoľahlivosti zamestnancov																
CIEĽ	Pochybenie v projekte		Prezentovanie podnikových informácií na verejnosti		5	Poškodenie mena spoločnosti		3	Zamestnanie v spoločnosti pre získanie informácií		2	Pochybenie v projekte		3		
	už zabehnutý zamestnanec	3	úmyselne	3		úmyselne	3		nový zamestnanec	2		nový zamestnanec	3			
UDALOSTI	17%		17%		4	20%		3	33%		1,33	20%		2,8		
	Spôsobené nedbalosťou	4	Dochádza ku definovaniu informácií?	4		Dochádza k preverovaniu a kontrole zamestnancov?	3		Dochádza k overovaniu potenciálnych zamestnancov?	2		Nedostatočné zaškolenie	3			
	Spôsobené nedostatočným preškolením	3	Dochádza k určeniu citlivosti informácií?	4		Je možné, že tretia strana by poskytla finančnú odmenu zamestnancovi za poškodenie?	4		Sú zamestnanci zaviazaní zmluvnými podmienkami k mlčanlivosti?	2		Sú zamestnanci preverovaní u bývalých zamestnávateľov?	1		Nedostatočné vedomosti	3
	Spôsobené nedostatočnými vedomosťami	2	Dochádza ku školeniam proti útokom soci. inžinierov?	4		Dochádza v spoločnosti ku externým nezhodám?	3		Dochádza k definovaniu pracovných postupov?	3		Dochádza k testovaniu záujemcov?	1		Nedostatočná certifikácia	3
	Cieľené poškodenie projektu	3	Dochádza ku určeniu manipulácií s informáciami?	4		Má spoločnosť zabezpečenú prácu s dátami?	5		Dochádza ku práci s citlivými údajmi?	2					Nedostatočné oboznámenie sa s pracovnými postupmi	3
	Chyba v projekte v dôsledku neverenia a kontroly	3	Je definovaný prístup zamestnancov k projektom?	3												

ZDROJ: (autor)

Hodnotenie spoľahlivosti zamestnancov je realizované na rovnakých funkčných princípoch, ale dochádza k definovaniu iných analytických otázok, ktoré z hľadiska primárneho cieľa úzko súvisia so skúmanou problematikou. Jedná sa o otázky súvisiace s pracovným výkonom, ktorých odpovede a ich následné hodnotenie štatisticky vyhodnocuje, pričom

dochádza k vzniku nedostatkov. Je všeobecne známe, že práve človek je v spoločnosti považovaný za najväčšiu hrozbu a z toho dôvodu, by malo dochádzať k stanoveniu opatrení, ktoré minimalizujú možné poškodenie zamestnancom, alebo konaním inej osoby.

4.1.5 Analýza kompetencií zamestnancov

Nasledujúca časť práce analyzuje súčasne definované pracovné miesta vzhľadom ku kompetenciám, ktoré jednotlivé miesta zastupujú, ale aj vzhľadom ku počtu osôb, ktoré zastávajú danú pozíciu. Uvedené hodnotenie je zostavené na základe pridelenia číselnej hodnoty pre hodnotenie pracovnej činnosti.

Tab. 15. Tabuľkové hodnotenie hodnotiacich pracovných pozícií

Hodnotenie pracovných činností	
Dohľad	4
Plné vedenie	3
Kontrola	2
Vykonanie určitej úlohy	1

ZDROJ: (autor)

Číselné hodnotenie je definované od najmenej hodnoty po najvyššiu, pričom hodnota 1 definuje, že uvedený pracovník, alebo daná pracovná pozícia má kompetenciu vykonať dotazovanú úlohu. Číselná hodnota 2 definuje kontrolu na prvej úrovni, vo väčšine prípadov sa jedná o kontrolovanie manažérom daného oddelenia. Plné vedenie reprezentuje hodnota 3, kedy dochádza ku kontrole na druhej úrovni a vedeniu celého procesu zameraného na danú úlohu. Dohľad, znamená, že daný pracovník je pracovník na najvyššej úrovni v danej úlohe a jeho funkcia reprezentuje dohľad nad všetkými dôležitými časťami projektu.

Uvedená analýza je dôležitá pre bezpečnosť, primárne pre určenie práv, ktoré sú určované pre manipuláciu s dátami a projektmi v spoločnosti a pre návrh informačného systému, ale aj ako východiskový materiál pre stanovenie pravidiel prístupového systému do jednotlivých objektov, ale hlavne miestností.

4.1.5.1 Obchodné oddelenie

Nasledujúca tabuľka vizualizuje nástroj na hodnotenie kompetencií obchodného oddelenia. Uvedené kompetencie vzhľadom k úlohám definujú účasť obchodného oddelenia, a teda

nedochádza ku prepojeniu úloh a pozícií s inými oddeleniami. Na záver tabuľky dochádza k uvedeniu prepojenia s inými oddeleniami.

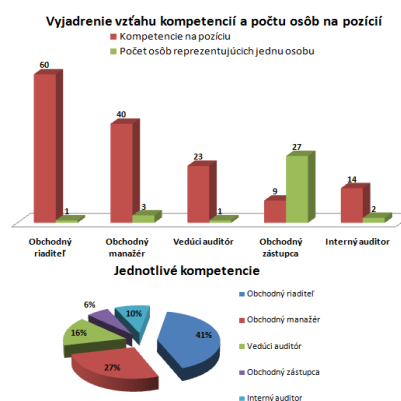
Tab. 16. Analytické hodnotenie kompetencií obchodného oddelenia

	Obchodný riaditeľ	Obchodný manažér	Vedúci auditór	Obchodný zástupca	Interný auditor
Hodnotenie					
Celkové kompetencie	60	120	23	243	28
Delonovanie kompetencií	60	40	23	9	14
Peet osôb v organizácii	1	3	1	27	2
Dodávateľia					
DODÁVATELIA zahraničný trh	4	3	2	1	
DODÁVATELIA tuzemský trh	4	3		1	
Klienti					
KLIENTI podnikateľské subjekty	4	3	2	1	
KLIENTI súkromné osoby	4	2		1	
Obchodné prvky					
Marketingové		2	2	1	3
Jednanie s klientmi		9		1	
Návrhy riešení	4	9		1	
Cenové kalkulácie		3		1	
Objednávky				1	
Kontrolovanie procesov					
Kontrolvanie interných procesov	4	2	3		1
Kontrolovanie zmluvných podmienok	4	2	3		1
Kontrola certifikácií	4	2	3		1
Kontrola dodržiavania požiadaviek	4	2	3		1
Iné					
Jednanie s inými oddeleniami	4	3			1
Jednanie s technikmy		3			1
Kntrola iných oddelení		4			3

ZDROJ: (autor)

Nasledujúce grafické vyhodnotenie reprezentuje jednotlivé pozície a kompetencie ku pozícií. Uvedené vyhodnotenie definuje závere, ktorý identifikuje dôležitosť jednotlivých pozícií. Ak sa na dané vyhodnotenie pozrieme formou percentuálneho vyjadrenia zistíme, že v prípade obchodného oddelenia má pracovná pozícia riaditeľa 40% všetkých kompetencií.

Graf 2. Grafické vyhodnotenie kompetencií obchodného oddelenia



ZDROJ: (autor)

4.1.5.2 Oddelenie bezpečnostného manažmentu

Pri analytickom procese oddelenia bezpečnostného manažmentu dochádza ku rozšírejšiemu popisu jednotlivých kompetencií, čo môže byť spôsobené tým, že dané služby sú najdlhšie poskytované uvedenou organizáciou.

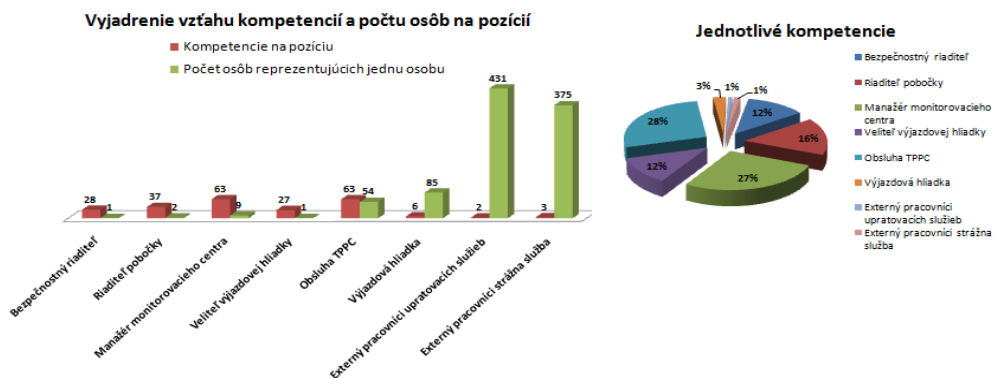
Tab. 17. Analytické hodnotenie kompetencií oddelenia bezpečnostného manažmentu

		Bezpečnostný riaditeľ	Riaditeľ pobočky	Manažér monitorovacieho centra	Veľiteľ výjazdovej hliadky	Obsluha TPPC	Výjazdová hliadka	Externý pracovník upratovacích služieb	Externý pracovník strážna služba
Hozborno	Celkové kompetencie	28	74	567	27	3402	510	862	1125
	Definovanie kompetencií	28	37	63	27	63	6	2	3
	Počet osôb v organizácii	1	2	9	1	54	85	431	375
Výsledie	Kontrola školení a vzdelávania	4	3	3	3				
	Riadenie monitorovacieho centra			4	3				
	Vedenie pracovných funkcií	4	3	3	3				
	Plánovanie splnenia zmluvných podmienok obchodných zmlúv	4	3	2	2				
Pracovný riaditeľ	Definovanie časového harmonogramu služieb		4	3	3				
	Definovanie pracovného výkonu strážneho	4		3					1
	Definovanie pracovného výkonu výjazdovej hliadky	4		3	3		1		
	Plánovanie nasadenia jednotlivých zamestnancov		4	3	2	1			
	Trénovanie a takticko operatívna príprava výjazdovej hliadky		4	2	3		1		
	Definovanie pracovného výkonu upratovacej služby			4		2		1	
Monitoringu stavu	Monitorovanie sledovaných objektov		4	3	2	1	1		
	Monitoring kamerových systémov		4	3		1			
	Monitoring dochádzkového systému		4	3		1			
	Kontrola vstupu do objektov			3			2		1
	Kontrola dodržiavania interných pravidiel v objekte			3	2	2	1	1	1
	Záznamy o stave objektov		4	3		1			
	Komunikácia s technickým oddelením a servis	4		3					
Pokyny pre iné oddelenia	4		3						

ZDROJ: (autor)

Grafické vyhodnotenie definuje záver, že na analyzovanom oddelení majú najnižšie kompetencie pracovníci upratovacích služieb, ale na približne rovnakej úrovni sa nachádzajú manažér monitorovacieho centra a obsluha TPPC vzhľadom na určené úlohy.

Graf 3. Grafické vyhodnotenie kompetencií oddelenia bezpečnostného manažmentu



ZDROJ: (autor)

4.1.5.3 Technické oddelenie

Technické oddelenie je najrozšírenejšie a v súčasnej dobe sa plánuje ešte jeho ďalší rast, ktorého potrebu zaznamenali aj jednotlivé analytické výsledky.

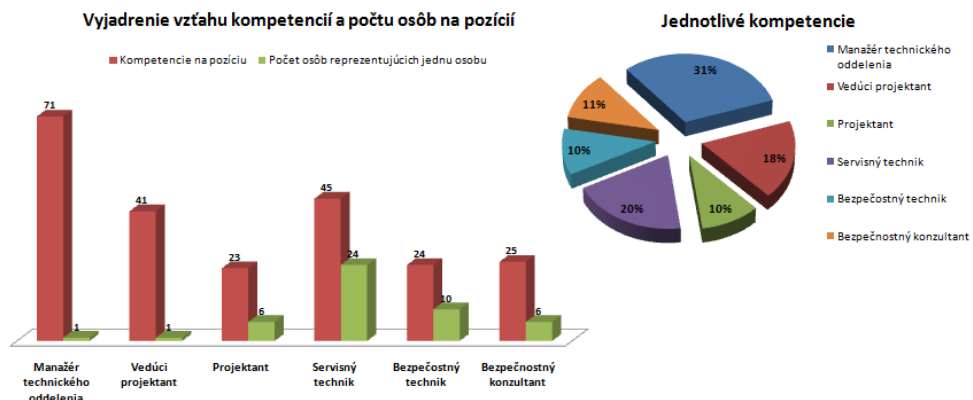
Tab. 18. Analytické hodnotenie kompetencií technického oddelenia

	Manažér technického oddelenia	Vedúci projektant	Projektant	Servisný technik	Bezpečnostný technik	Bezpečnostný konzultant
Celkové kompetencie	71	41	138	1080	240	150
Definovanie kompetencií	71	41	23	45	24	25
Počet osob v organizácii	1	1	6	24	10	6
Vedenie projektu	4	3				
Kontrola právnych predpisov	4	3				
Kontrola technických noriem	4	3				
Kontrola školení a kvalifikácie	4					
Definovanie potreby na pracovníkov upratovacej služby		4				
Definovanie potreby bezpečnostných pracovníkov		4				
Analytické činnosti	Technické návrhy riešení pre klienta		2		1	
	Návrh komponentov jednotlivého zabezpečenia		2		1	
	Návrh riešenia komunikácie		2		1	
	Návrh prevádzkových pravidiel		2			1
	Návrh kontrolných opatrení		2	1	1	
	Odôvodnenie riešenia		2			
Inštaláčne činnosti	Časový harmonogram inštalácie systému	3	1	1	1	2
	Určenie technikov zakomponovaných do inštalácie	4		1	1	3
	Určenie dodávky technickej montáže v prípade externého dodávateľa	3				1
	Určenie dohľadu nad inštaláciou	4				3
	Určenie dokumentácie k inštaláciám	4	3	1		
	Určenie uloženia pracovných postupov	4	3		1	1
	Definovanie postupov inštalácie	3			1	
	Definovanie potreby vyjadrenia iného oddelenia	2				1
Servis	Definovanie pravidelných servisných kontrol	4		2	1	1
	Definovanie postupov v prípade zlyhania tech. komponentu			3	2	
	Definovanie postupu v prípade prerušenia prenosovej cesty			3		1
	Zabezpečenie servisovaného miesta			3		1
	Plánovanie opravy havárie			3		1
	Riešenie reklamácií komponentov				3	1
	Dokumentácia servisných činností			3		2
Monitoring	Monitorovanie nahrávacieho systému z objektov		3			Komunikácia s manažérom monitorovacieho centra
	Monitorovanie a hodnotenie prístupových údajov		3			Komunikácia s manažérom monitorovacieho centra
	Monitorovanie sledovaných objektov		3			Komunikácia s manažérom monitorovacieho centra
	Pokyny pre iné oddelenia a servis	Komunikácia s manažérom monitorovacieho centra				
	Záznamy o stavoch objektov					Komunikácia s manažérom monitorovacieho centra
	Výjazd hliadky k objektu	Oddelenie bezpečnostného manažmentu				
Vedenie výjazdovej hliadky						

ZDROJ: (autor)

Vyhodnotením dochádzame k záveru, že absenciou riadiaceho pracovníka na technickom oddelení, teda riaditeľa technického oddelenia, dochádza k presunu kompetencií na manažéra technického oddelenia. Technické služby sú rozsiahle a je nutné dbať na ich správnu funkciu, pretože v prípade poškodenia dochádza k nefunkčnosti celého systému, a tým k nespokojnosti klienta, až môže dôjsť k strate zákazníka.

Graf 4. Grafické vyhodnotenie kompetencií oddelenia bezpečnostného manažmentu



ZDROJ: (autor)

V prípade, že hovoríme o technických pracovných pozíciách je nevyhnutné definovať požiadavky na znalosti, vedomosti a skúsenosti vzhľadom k pracovnému výkonu povolania. Uvedené aspekty budú podľa potreby navrhované v návrhovej časti práce.

4.1.5.4 Oddelenie informačných technológií

Oddelenie informačných technológií nie je v súčasnej dobe definované, a jeho funkcia je len v plánovaní a prvotnom zavádzaní do procesu chodu organizácie. Oddelenie informačnej bezpečnosti je ale veľmi dôležité, vzhľadom na budúci vývoj firmy, a to z dôvodu, že v súčasnosti organizácia poskytuje také technické zabezpečenie, ktoré pracuje s údajmi, ktoré daná organizácia musí, alebo by minimálne mala vyhodnocovať. Jeden z ďalších dôvodov je neustály rast potreby zavádzania informačných systémov do chodu organizácií, a teda aj ochrana dát, ktoré sú v daných informačných systémoch spracovávané. V neposlednom rade zohráva veľkú úlohu rast hodnoty informácií pre podniky a spoločnosti.

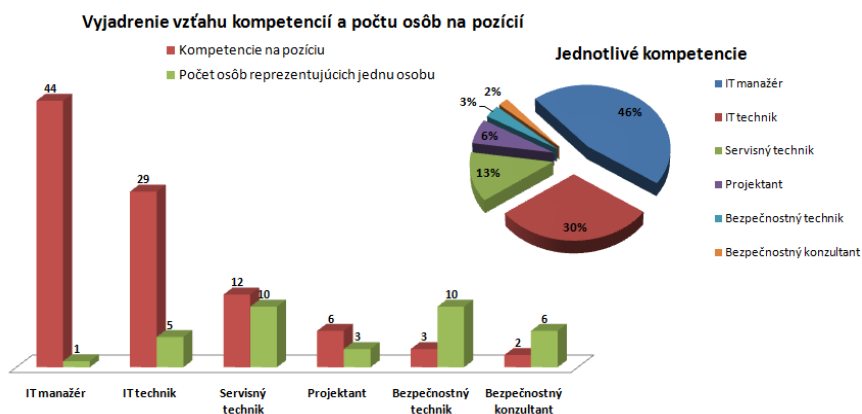
Tab. 19. Analytické hodnotenie kompetencií IT oddelenia

		IT oddelenie		Vázy iných zamestnancov na dané oddelenie			
		IT manažér	IT technik	Servisný technik	Projektant	Bezpečnostný technik	Bezpečnostný konzultant
Hodnotenie	Celkové kompetencie	44	145	120	18	30	12
	Definovanie kompetencií	44	29	12	6	3	2
	Počet osôb v organizácii	1	5	10	3	10	6
	Definovanie časového harmonogramu	4					
Potreby pre zariadenia	Vedenie IT oddelenia	4	3				
	Analýza potreby IS	3			2	1	1
	Návrh IS pre klienta	3	3		2	1	
	Kontrola funkčnosti a plnenia úlohy IS	4	3	2			
	Doplnenie prepajení IS	4	2	1			
	Vyhodnocovanie zmien v IS	4	3	2			
	Aplikácia nových zmien do IS	4	3	2			
	Nastavovanie väzieb v IS	4	3	2			
	Kontrola plnenia úloh	4	3				
	Definovanie potreby školení	4	3	3	2	1	1

ZDROJ: (autor)

V prípade vyhodnotenia dochádza k zisteniu, že na tvorbe jednotlivých procesov sa podieľajú spolupracovníci z iných oddelení, ale samozrejme najvyššie kompetencie dosahujú pracovníci, ktorí sú definovaní funkciou špecializovanou na informačné technológie.

Graf 5. Grafické vyhodnotenie kompetencií oddelenie informačných systémov



ZDROJ: (autor)

Najnižšiu úroveň kompetencií z hľadiska IT systémov má bezpečnostný konzultant, ktorého úlohou je rozumieť základným výhodám a funkciám uvedeného systému, a to pre potreby návrhu pre klienta. Bezpečnostný konzultant by mal dané technické špecifikácie vedieť vysvetliť jednoducho a laickým spôsobom.

4.1.5.5 Personálne oddelenie

Personálne oddelenie je definované primárne dvoma pracovnými funkciami, ale dochádza k participovaniu iných pracovných pozícií na zostavovaní daných procesov personálneho oddelenia, a to primárne z dôvodu, že oddelenie definuje požiadavky na pracovníkov, ako výberové pohovory, ale aj kontrolne opatrenia a iné funkcie, ktoré vzájomné prepojenie vyžadujú.

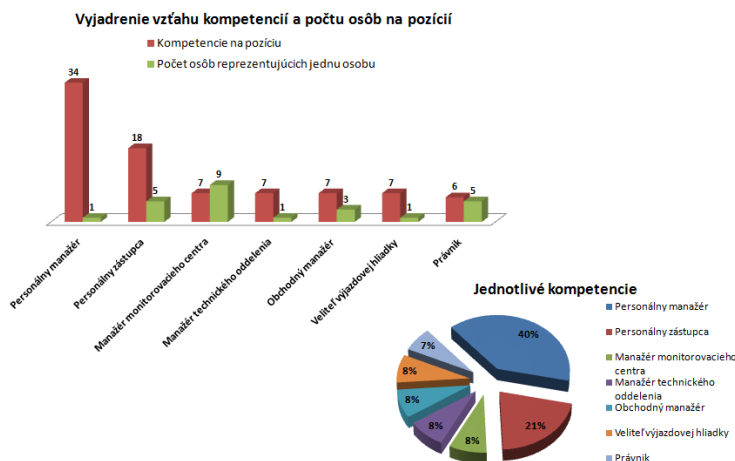
Tab. 20. Analytické hodnotenie kompetencií personálneho oddelenia

		Personálne oddelenie		Vedenie iného oddelenia				
		Personálny manažér	Personálny zástupca	Manažér monitorovacieho centra	Manažér technického oddelenia	Obchodný manažér	Veliteľ výjazdovej hliadky	Právnik
Hodnotenie	Celkové kompetencie	34	90	63	7	21	7	30
	Definovanie kompetencií	34	18	7	7	7	7	6
	Počet osôb v organizácii	1	5	9	1	3	1	5
Požiadavky	Definovanie pracovných pozícií		3	1	1	1	1	
	Definovanie kvalifikačných požiadaviek	4	3	1	1	1	1	2
	Definovanie procesu vzdelávania a školenia	3	2	1	1	1	1	1
	Časový harmonogram školení	3	2					
Výberové konanie	Výberové konania 1. kola	4	2	1	1	1	1	
	Výberové konania 2. kola		2	1	1	1	1	1
	Definovanie výberových dotazníkov		2	1	1	1	1	
	Definovanie procesu prijatia do výkonu povolania		2					
Práve a ekonomické	Definovanie zmlúvnych podmienok	4		1	1	1	1	1
	Definovanie ekonomických požiadaviek							1

ZDROJ: (autor)

Podobne ako v prípade IT oddelenia, najvyššie kompetencie majú pracovníci uvedeného oddelenia, vzhľadom na to, že jednotlivé procesy riadia. Participovanie na výstavbe personálnych požiadaviek je veľmi dôležitý aspekt pre výber vhodných osôb zastávajúcich jednotlivé pozície.

Graf 6. Grafické vyhodnotenie kompetencií personálneho oddelenia



ZDROJ: (autor)

Z uvedených zistení bude následne dochádzať ku návrhu prístupových práv, ale aj práv pre prácu s projektmi, ktoré sú predmetom poskytovania služieb pre zákazníka. Pre správne určenie bezpečnostnej politiky je veľmi dôležité podrobné pochopenia procesov, ktoré prebiehajú ako na internej, tak na externej úrovni.

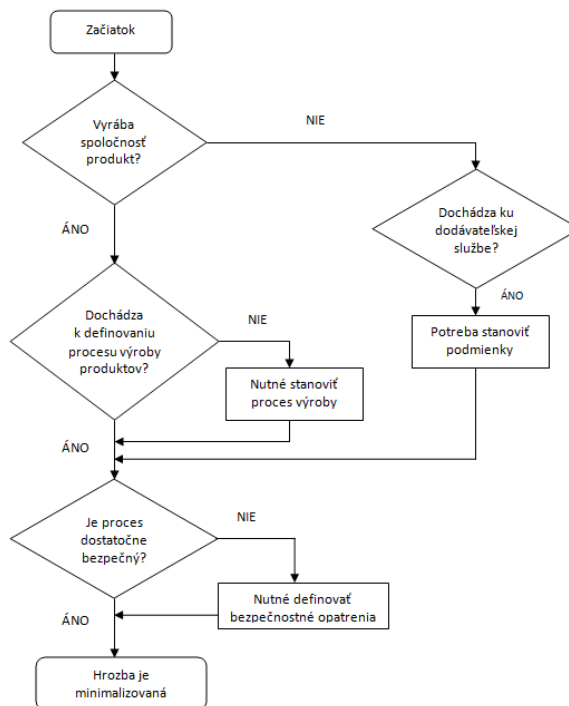
4.2 Bezpečnostná prognóza

Nasledujúca časť práce popisuje prognózovanie stavu organizácie, pričom dochádza k využitiu modelovania jednotlivých situácií, ktoré v podniku hrozia. Organizácia uviedla, že v súčasnosti nedochádza ku výrobe komponentov, ale do budúcnosti by vedenie organizácie chcelo vytvoriť vlastné komponenty, ktoré by pre inštaláciu využívali, teda by nedochádzalo k dodávke komponentov na zabezpečenie od dodávateľských firiem, ale produkty by boli vyrábané spoločnosťou. Uvedený prognostický cieľ je orientovaný do budúcnosti a v prvej úrovni by dochádzalo ku výrobe externou službou, ktorá by spĺňovala určené požiadavky. Uvedený cieľ je ale dlhodobý a v súčasnosti nie je predmetom našej bezpečnostnej prognózy, ale je veľmi dôležité si to uvedomiť v prípade dlhodobých plánov.

Podnikateľský subjekt pracuje s veľmi citlivými údajmi o spoločnostiach klientov, a teda je nutné jeho funkcie ochraňovať na vnútornej, ale aj vonkajšej úrovni. Ak by došlo ku zverejneniu údajov, bola by to kategoricky najhoršia možná voľba, ktorá by nastala, a to z dôvodu, že uvedeným incidentom by spoločnosť úplne stratila svoju cenu a predmet podnikania. Uvedená hrozba, je v našom prípade považovaná za najrizikovejšiu, a to z dôvodu, že spoločnosť je orientovaná na poskytovanie bezpečnostných služieb.

V uvedenej organizácii dochádza ku sústredeniu pracovných pozícií, ktoré sú definované v segmente bezpečnostného manažmentu. V uvedenom sektore je nutné presne definovať výkon pracovnej pozície, a to z dôvodu, že pochybenie pracovníkov by taktiež mohlo viesť ku katastrofickému scenáru a zničeniu spoločnosti. Každá udalosť, ktorá by viedla ku zániku alebo zničeniu organizácie je reprezentovaná na najvyššom stupni krízovej pyramídy, a to v paralelnom vzťahu. Medzi ďalšiu z uvedených hrozieb, ktoré pôsobia deštruktívne je práca s informáciami. V súčasnej dobe hodnota informácií rastie, a hlavne v sektore bezpečnostných služieb je nutné si uvedený aspekt uvedomiť a stanoviť pravidlá pre prácu na projektoch, ako aj definovať právne predpisy, ktoré je nutné dodržiavať.

Nasledujúci diagram popisuje základný proces modelovania v analyzovanej organizácii, ktorý je možné aplikovať pre ďalšie služby v rámci interných procesov organizácie.



Obr. 45. Využitie diagramu pre modelovanie

ZDROJ: (autor)

Uvedený diagram reprezentuje možné využitie, ako modelovací prostriedok pre definovania budúceho vývoju v určitých prípadoch. Uvedený modelovací prístup je možné využívať aj na definovanie postupov v organizácii, pretože sa jedná o jasné a stručné určenie procesov do budúcnosti. Jedná sa o prepojenie s prognózovaním, pretože dochádza k prognóze, kedy

na jednej strane je otázka, čo ak daná udalosť nastane a na strane druhej je odpoveď, ktorá vedie k jedinému cieľu.

4.3 Definovanie záverov

Časť práce pod názvom definovanie záverov, popisuje a zhodnocuje celý analytický proces, ktorým daná organizácia prešla za účelom návrhu bezpečnostnej politiky organizácie. Jedná sa o vyslovenie hlavných záverov, na ktoré by sa mala bezpečnostná politika zameriavať. V prípade, že riešenie je časovo náročné dochádza k určeniu krokov, ktoré v určitom časovom intervale budú naplňovať vyslovený cieľ, ktorý je výsledkov uvedených analýz.

Jednotlivé analytické nástroje, ktoré boli v predchádzajúcej časti popísané definujú aj výsledky analytického procesu. Nasledujúca tabuľka znázorňuje len základné potreby, ktoré by mala uvedená bezpečnostná politika splňovať.

Tab. 21. Vyhodnotenie analytického procesu

Vyhodnotenie analytického procesu			
Primárne potreby	Dokumentácia	Časový harmonogram	Kontrolne dokumenty
Definovať fyzické zabezpečenie objektu	áno		áno
Definovať priestorové a stavebné dispozície	áno		áno
Definovať kontrolné opatrenia a monitoring	áno	áno	áno
Definovanie požiadaviek na jednotlivé pracovné pozície	áno		kontrola výkonu pracovnej náplne
Definovanie požiadaviek na BOZP	áno		áno
Definovanie požiadaviek a časový plán pre zavádzanie ISO 9001	áno		vyžadované normou
Definovanie návrhu pre zavedenie informačného systému	áno	časový plán vývoja	Zatiaľ nie - jedná sa o návrh funkčnosti
Definovanie prístupových úrovní	áno	určenie časového intervalu prístupu	záznamy o prístupe
Definovať pracovné postupy	áno	možný odhad časového intervalu potrebného na vykonanie	nutná kontrola
Definovať interval odchýliek	áno		áno
Definovať proces vzdelávania	áno	plánovanie	testy
Definovať proces reklamácie	áno	definovanie intervalov možnej reklamácie	záznamy o reklamácií

ZDROJ: (autor)

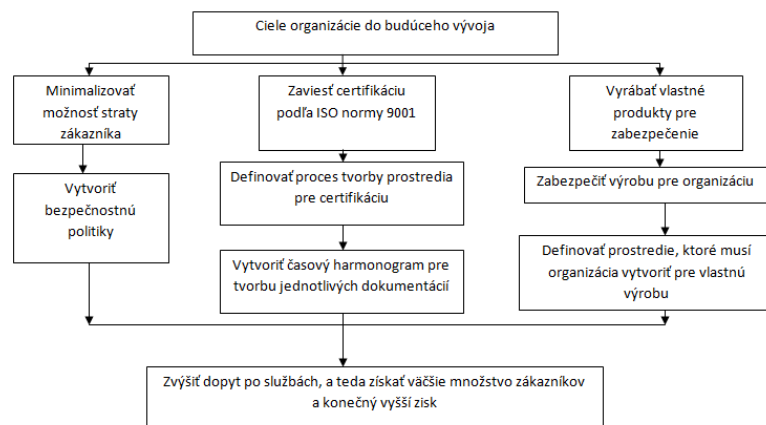
Základný dokument by mal definovať ciele organizácie, ktoré by mali byť nemenné a následne by malo dôjsť k stanoveniu prostriedkov, ktoré budú naplňovať vytýčené ciele. Prostriedky na dosiahnutie cieľa sa v čase môžu obmieňať podľa prostredia, v ktorom sú aplikované.

5 NÁVRH BEZPEČNOSTNEJ POLITIKY PODNIKU

Návrh bezpečnostnej politiky definuje základný dokument, ktorý v rámci podnikateľského subjektu patrí medzi hlavné dokumenty, ktorými by mala byť organizácia riadená. Jedná sa primárne o tri druhy bezpečnostných opatrení, a to bezpečnosť procesov, technická bezpečnosť a personálna bezpečnosť. Konečným cieľom bezpečnostnej politiky je vytvorenie záväzného dokumentu, ktorý bude vytvárať bezpečné prostredie na chod organizácie.

5.1 Definovanie stratégie

Nasledujúca časť práce definuje základné stratégie, ktoré by mali byť do budúcnosti podniku aplikované za určitým dosiahnutím cieľa. Jednotlivé stratégie by mali byť zohľadňované pri definovaní bezpečnostnej politiky, a to z dôvodu, aby nedochádzalo ku ich negácií pravidlami bezpečnostnej politiky.



Obr. 46. Zobrazenie základných strategických cieľov do budúceho vývoja organizácie

ZDROJ: (autor)

Uvedené strategické ciele, definujú základný cieľ zvýšiť prestíž organizácie, a tým aj svoj zisk a eliminovať negáciu cieľa. Stratégia je spôsob, ktorým dôjde k naplneniu cieľa, teda je to postupnosť určených krokov, ktoré po ich aplikácií do praxe by mali uvedený cieľ naplniť.

Pre naplnenie strategických cieľov dochádza k použitiu jednotlivých stratégií, medzi ktoré patria nasledujúce stratégie, ktoré chce uvedená organizácia aplikovať pre dosiahnutie cieľa:

- Stratégia určenia potrebnej dokumentácie,
- Stratégia plánovania,
- Stratégia spätnej väzby od zákazníkov,
- Stratégia zvyšovania kvality poskytovaných služieb,
- Stratégia kontroly a vyhodnocovania,
- Stratégia plánovania inovácií.

Uvedené strategické postupy sú využívané pre naplnenie uvedených cieľov a pre stanovenie nasledujúcich opatrení a definovanie interných smerníc.

5.2 Definovanie smerníc pre zavedenie fyzickej bezpečnosti objektu

Uvedené smernice charakterizujú základné ciele pre zabezpečenie jednotlivých stavebných objektov, v ktorých organizácia vykonáva svoju činnosť. Základným cieľom je zabezpečiť budovu a priestory, v ktorých sú vykonávané jednotlivé pracovné funkcie.

POSTUP pre zahájenie bezpečnostného projektu:

1. V prípade, že zodpovedná osoba (manažér monitorovacieho centra, riaditeľ pobočky, manažér technického oddelenia) identifikuje nedostatok v oblasti fyzickej bezpečnosti objektu, dochádza k vypracovaniu návrhu na zmenu.
2. Návrh na zmenu je podaný v písomnej podobe a dochádza k definovaniu spôsobu, ktorým bol odhalený nedostatok na zabezpečení, následne je definovaný žiaduci stav a navrhovaný spôsob riešenia spolu s odhadom finančnej náročnosti.
3. Uvedený dokument Návrh na zmenu fyzickej bezpečnosti je prednesený na porade vedenia.
4. Porada vedenia má za povinnosť preriešiť adekvátnosť riešenia situácie a stanoviť jeho prioritu, a to v termíne do 14. dní od podania návrhu.

5. V prípade, že dôjde k záveru, že daný návrh je adekvátny a je potrebné ho riešiť, dochádza k zvolaniu špeciálneho tímu, ktorý určí osoby, ktoré sa na danom projekte budú podieľať aj s určením zodpovedností a kompetencií.
6. Následne dochádza k určeniu časových intervalov, v ktorých je nutné danú úlohu vykonať a taktiež definuje perioditu kontroly. Uvedené časové intervaly definujú zodpovedný pracovníci za uvedenú úlohu.
7. Dochádza k vypracovaniu celého projektu a určitých častí, ktoré schvaľujú nadriadení pracovníci. Následne dochádza k schváleniu celého projektu na porade vedenia.
8. Dochádza k inštalácii, alebo zavedeniu uvedeného systému. Zavedenie systému je zložené z fáze dodávky materiálu, inštalácia systému, vypracovanie dokumentácie, vypracovanie záznamových dokumentov, vypracovanie skúšobných dokumentov a iné potrebné pre prevádzku.
9. Po dokončení inštalácie je prevedená kontrola funkčnosti a dochádza k zahájeniu skúšobnej prevádzky systému. Dochádza k záznamu všetkých nezrovnalostí v systéme, ktoré sú následne odstránené.
10. Určenie servisných opatrení a plánovanie kontrol funkčnosti systému.
11. Zahájenie trvalej prevádzky systému.
12. Vykonávanie určených kontrol v časovom intervale podľa projektu.

Uvedený postup je rovnaký pre každé oddelenie organizácie. K zmene dochádza podľa úrovne, ktorej sa dotýka daná zmena a podľa určeného vedenia projektu. Ak chceme aby definovaný postup fungoval, je nutné do procesu zaviesť systém kontroly, ktorý bude analyzovať funkčnosť systému, s tým že dôjde k návrhu určitých zmien práve od vedúcich pracovníkov. Tu je viditeľné, že vedúci pracovníci musia byť dostatočne vzdelaný, aby došlo k identifikácii potreby zmeny.

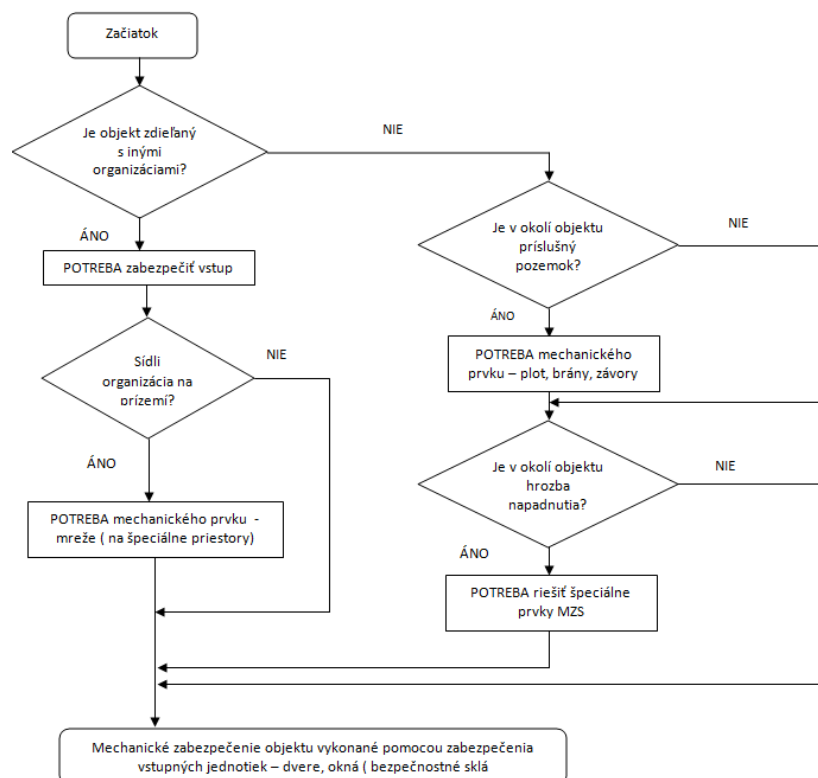
5.2.1 Mechanické zábranné systémy

Každý z objektov uvedenej organizácie musí spĺňať nasledujúce podmienky, ktoré definuje uvedené prostredie v ktorom sa daný objekt nachádza.

Prvky mechanického zabezpečenia:

- Oplotenie,
- Brány a závory,
- Mreže a rolety,
- Zámky,
- Úschovné objekty,
- Bezpečnostné dvere, fólie a sklá.

Pre inštaláciu uvedených prvkov dochádza k rozhodovaciemu procesu, ktorý určí aké jednotky je nutné pre daný objekt inštalovať. Vychádza sa z uvedeného diagramu, ktorý určuje, podľa akých kritérií dochádza k rozhodovaniu, či daný objekt bude mať definovaný daný mechanický prvok pre vonkajšiu ochranu.



Obr. 47. Diagram hodnotenia nasadenia uvedených mechanických prvkov do objektu organizácie

ZDROJ: (autor)

Z hľadiska mechanického zabezpečenia objektu je vzhľadom na povahu organizácie vždy nutné definovať vstupné bezpečnostné dvere, pokiaľ sa jedná o presklené otvory, je nutné navrhnuť sklá, ktoré sú vzhľadom k objektu najvhodnejšie, jedná sa o tvrdené, alebo

vrstvené sklá. V prípade, že objekty už majú definované sklenené výplne a nie je prijateľné dané sklá meniť z dôvodu finančnej náročnosti, dochádza ku lepeniu bezpečnostných fólií. V prípade vstupných dverí je doručované vzhľadom k povahe podnikania použiť taktiež bezpečnostné dvere, ako aj mreže.

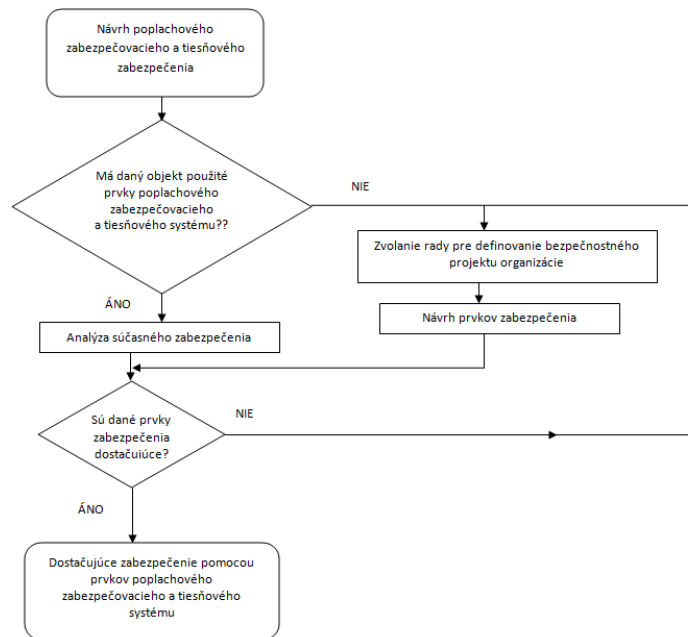
V uvedených objektoch je nutné definovať aj úschovné objekty. Medzi uvedené patria trezory, komorové trezory, trezorové skrine a depozitné systémy. Uvedené systémy sa vo väčšine prípadov dopĺňujú o ďalšie technické prostriedky ochrany, predovšetkým o napojenie na elektronický zabezpečovací systém a elektronickú požiarňu signalizáciu.

Zásady zabezpečenia objektu mechanickými zábrannými systémami:

1. Každý objekt, ktorý patrí organizácii a dochádza v ňom ku vykonávaniu určitej úlohy organizácie musí mať mechanické zábranné prvky.
2. Ak uvedený objekt disponuje areálom, je nutné, aby bol oplotený a vjazd do objektu musí byť zabezpečený závorou.
3. Ak miesto pre výkon určitej funkcie podniku je sústredené v budove, v ktorej sídli aj iné spoločnosti, je nutné, aby došlo k oddeleniu celého poschodia a zároveň vchod na dané poschodie musí byť opatrený vstupnými dverami.
4. Ak v príslušnej budove sídli len uvedená spoločnosť, je nutné aby daný objekt bol zabezpečený bezpečnostnými vstupnými dverami a bezpečnostnými fóliami.
5. Ak dochádza k umiestneniu rizikových priestorov do prízemí, je nutné, aby dané rizikové priestory boli zabezpečené mrežami na okenných otvoroch.
6. Každý vybraný objekt, ktorý slúži na prevádzku uvedenej organizácii musí byť zabezpečený a jeho rozsah je schvaľovaný vedením organizácie.

5.2.2 Poplachový zabezpečovací a tiesňový systém

Každý z uvedených objektov, ktorý je súčasťou uvedenej spoločnosti má definovaný základný rámec elektronického zabezpečenia objektu. Jedná sa o elektronickú zabezpečovaciu signalizáciu a elektrickú požiarňu signalizáciu.



Obr. 48. Diagram hodnotenia nasadenia prvkov poplachového zabezpečovacieho a tiesňového systému

ZDROJ: (autor)

Uvedený diagram je navrhovaný pre hodnotenie súčasného systému jednotlivých objektov, jedná sa o popis úloh, ktoré majú prejsť v prípade, že dané zabezpečenie nie je dostačujúce pre výkon uvedených úloh.

Zásady zabezpečenia objektu poplachovými a tiesňovými prvkami:

1. Priestory určené na vykonanie určitej úlohy organizácie, musia vždy splňovať podmienky technického zabezpečenia.
2. Každé monitorovacie centrum, ale aj riadiaca pobočka musí mať definovaný tiesňový poplachový zabezpečovací systém, ktorý sa skladá z detektorov, ústredne, klávesnice a koncových signalizačných zariadení.
3. Každý uvedený systém musí detekovať a signalizovať narušenie v určitých časových intervaloch.
4. Každý uvedený systém musí disponovať záložným zdrojom a funkčnou prenosovou cestou.
5. V prípade uvedeného systému nesmie dochádzať k jeho negatívnemu ovplyvňovaniu iným systémom.

6. Funkčnosť uvedeného systému musí byť pravidelne kontrolovaná a kontrola musí byť vyhodnocovaná a zaznamenávaná.
7. Každý objekt musí mať definované zóny podľa stupňa stráženia.
8. Uvedený systém musí byť definovaný projektovou dokumentáciou a súčasne musia byť určené postupy v prípade určitých udalostí.
9. Za uvedený systém v prevádzke musí byť stanovená zodpovedná osoba.

N základe vyššie uvedeného postupu dochádza ku definovaniu jednotlivých podmienok zabezpečenia daného objektu. Keďže daná organizácia rieši zabezpečenie svojich klientov, pre ich vlastné zabezpečenie dochádza k zvolaniu rady pre interné bezpečnostné systémy, ktorá určí zodpovedné osoby, ktoré majú kompetencie na návrh alebo hodnotenie daného systému.

5.2.3 Kameraný systém

Uvedené objekty momentálne nemajú definovaný kamerový systém. Pre zvýšenie bezpečnosti je navrhované, aby bol kamerový systém inštalovaný hlavne v priestoroch, kde dochádza ku všeobecnému pohybu osôb. Jedná sa o monitoring vnútorných priestorov.

Návrh kamerového systému:

- Navrhovaný kamerový systém by mal zaznamenávať udalosti vo vnútri objektu – voľne prístupné priestory (chodba).
- Navrhovaný systém by mal zaznamenávať a ukladať nahrávanie minimálne jeden týždeň.
- Uvedený záznam by mal byť monitorovaný mimo uvedený objekt, v ktorom dochádza ku monitoringu.

POSTUP pre projekt zavedenia kamerového systému:

1. Každá kamerová jednotka musí mať záložný zdroj.
2. Každá kamerová jednotka musí mať dokumentované parametre, ktoré budú charakteristické pre podmienky použitia (uhol záberu a dosah).
3. Systém prenosovej cesty bude plne funkčný bez obmedzení.

4. Záznam musí byť kontrolovaný a zaznamenávaný.
5. Zavedenie kamerového systému musí disponovať s dokumentáciou.
6. Dokumentácia musí definovať zodpovedné osoby a ich kompetencie.
7. Objekt musí byť vybavený výstražnými ceduľami, ktoré informujú o monitorovaní uvedeného systému.
8. V prípade, že vzniká oznamovacia povinnosť, je poverená osoba zodpovedná za oznámenie snímania verejného priestoru kamerovým systémom zo záznamom.

V prípade zmeny kamerového systému musí dochádzať ku zaznamenávaniu každej zmeny, a to prostredníctvom dokumentu „Záznam o zmene kamerového systému“. Tak ako iný systém musí byť aj kamerový systém pod servisnou kontrolou a v projekte sú presne definované osoby, ktoré sú zodpovedné za servis zariadení.

5.2.4 Kontrolne dokumenty pre správnu funkčnosť systému

Návrh na zmenu fyzického zabezpečenia je dokument, ktorý je spisovaný pred samotným návrhom zmeny zabezpečenia objektu. V dokumente dochádza ku základnej klasifikácii zmeny a primárnemu vyjadreniu sa k prínosu uvedenej zmeny do procesu. Hodnotenie je realizované za pomoci piatich hodnotiacich slovných spojení, ktoré sú reprezentované číselným hodnotením podľa dôležitosti, alebo hrozby, ktorú dané nedostatky spôsobujú.

Tab. 22. Hodnotenie návrhu na zmenu fyzickej bezpečnosti objektu

Slovné spojenie hodnotenia	Číselná hodnota	Vysvetlenie
ÁNO	5	Uvedená hrozba bezprostredne hrozí, alebo sa jedná o vykonanie uvedenej úlohy pri zmene
Čiastočne áno	4	K naplneniu uvedenej skutočnosti nedochádza v plnom rozsahu ale len čiastočne
Ano aj	3	Cieľ danej zmeny je iný, ale naplňuje aj uvedené požiadavky - sekundárne
Skôr nie	2	Uvedená hrozba bezprostredne nehrozí, a danú úlohu je potrebné vykonať len okrajovo
NIE	1	Dané riziko je už minimalizovaná a účel zmeny je iný

ZDROJ: (autor)

Nasledujúca tabuľka definuje základné atribúty, ktoré by mali byť hodnotené pri návrhu zmeny. Uvedený dokument by mal byť spísaný v prvej fáze, keď dochádza k uvedeniu potreby zmeny a návrhu. Následne dochádza ku doplneniu návrhu, teda k uvedeniu zodpovednou osobou a definovaniu konkrétnych požiadaviek na ďalšiu dokumentáciu, tým

pádum dochádza ku posunutiu návrhu do fáze rozhodovacej, v ktorej bude následne zvolaná rada, ktorá sa k danému návrhu vyjadrí, poprípade schváli obmedzenia. Pri zasadaní rady dochádza k uvedeniu základných termínov, ktoré musia byť dodržané pri zavádzaní zmeny do procesu realizácie.

Tab. 23. Dokument návrh na zmenu fyzického zabezpečenia objektu

Návrh na zmenu fyzického zabezpečenia objektu							
Meno a priezvisko podávajúcej osoby :							
Funkcia v organizácii :							
Sektor zmeny:				OBJEKT:			
Dôvod návrhu:							
Dátum podania návrhu				Dátum vyjadrenia			
Dátum predbežného vyjadrenia							
Hodnotenie		ÁNO	Čiastočne áno	Áno aj	skôr nie	NIE	HODNOTENIE
Dochádza k narušeniu bezpečnosti objektu?		5					12
Hrozí riziko vniknutia cudzej osoby do objektu?			4				
Je nefunkčný prvok zabezpečenia?				3			
Zmena							
Dotýka sa výmeny komponentov?				3			16
Dochádza ku návrhu doplnkových zariadení?				3			
Je finančne náročná daná zmena?				3			
Uvedená zmena je nevyhnutná pre naplnenie požiadaviek certifikácie?				3			
Je uvedená zmena vyžadovaná zákazníkom?			4				
Definovanie návrhu zmeny:							
Ako dlho by mala byť realizovaná náprava?							
Vyjadrenie:							
Zvolanie rady:	áno	nie	Termín rady:				
Zúčastnené osoby (funkcia/ meno)				Nutné dokumenty dodať			
Termín pre opravu návrhu:							
Zodpovedná osoba:							

ZDROJ: (autor)

Záznam o dokumentácii je dokument, ktorý charakterizuje primárne podmienky dokumentácie, jedná sa o rýchly kontrolný zoznam, ktorý identifikuje základné časti

dokumentácie pri návrhu projektu. Podľa jednoduchých otázok dochádza k presnej identifikácii cieľa projektu.

Tab. 24. Návrh dokumentu Záznam o dokumentácii

Záznam o dokumentácii							
Dátum začiatku projektu	Zodpovedné osoby					Osoby oprávnené k nahliadnutiu	
Predpokladaný termín ukončenia projektu	Meno a priezvisko		Pozícia	ZODPOVEDNOSŤ			
			obchodný zástupca	2			
			projektant	1			
			bezpečnostný konzultant	3			
			bezpečnostný technik	3			
			servisný technik	2			
Predpokladaný termín realizácie	Nákup techniky		ÁNO / NIE	Potreba bezpečnostného personálu	ÁNO / NIE	Dokumentácia s citlivými údajmi	ÁNO / NIE
	Zmeny v projekte					Druh citlivých údajov	
Dátum	Osoba rozhodujúca o zmene	Druh zmeny	Termín realizácie	Podpis	Návody k použitiu	ÁNO / NIE	
					Návrhy prevádzacích dokumentov	ÁNO / NIE	
					Definované postupy pre personál	ÁNO / NIE	
					Záznamy od klienta	ÁNO / NIE	
					Definované kontrolné procesy	ÁNO / NIE	
					Dochádzalo k porušeniu postupov	ÁNO / NIE	
					Dochádzalo k porušeniu termínov	ÁNO / NIE	
					Podpis zodpovednej osoby		

ZDROJ: (autor)

Uvedený dokument nie je hodnotiaci, preto nedochádza ku uvedeniu hodnotiaceho postupu, jedná sa o dokument zaznamenávajúci základné pracovné náplne celej dokumentácie v prípade získania zákazky. Uvedený druh dokumentu môže byť používaný aj na kontrolne preverky.

5.3 Definovanie smernice pre prístupový systém

Definovanie smerníc pre prístupový systém pozostáva z definovania jednotlivých pravidiel, ktorými by mal byť prístupový systém spoločnosti riadený, jedná sa o riadenie prístupov do jednotlivých kancelárií, skladov oddelení, ale aj do iných miestností a zasadacích a konferenčných sál.

Tab. 25. Hodnotenie pre kontrolu základných funkcií prístupového systému

Požiadavky na prístupový systém						
Objekt:						
Lokalizácia:						
Stav prístupového systému:		OK	CHYBY	ZMENA	NEGATÍVNE pôsobenie	
	ČO?	Zodpovedná osoba	spĺňa v rozsahu 99% - 75%	spĺňa v čiastočnom rozsahu 74% - 50%	nesplňuje ale je plánované menej ako 50%	nesplňuje rozsah menej ako 25% v procese plánovania
Základné funkcie	chrániť objekt pred cudzím konaním					
	chrániť objekt pred neoprávneným vstupom					
	chrániť informácie a materiál					
	kontrolovať vstup do miestnosti					
	kontrolovať pracovný čas zamestnancov					
	monitorovať pohyb osôb v objekte					

ZDROJ: (autor)

Každé z definovaných pracovísk musí spĺňať uvedené základné podmienky a malo by dochádzať k pravidelným kontrolám ich funkčnosti. Prístupový systém bude zavádzaný v objektoch s nasledujúcou prioritou podľa dôležitosti oddelení.

Nasledujúci návrh definuje priority pre zavedenie prístupového systému do objektov, jedná sa o riadiace pobočky, po inštalácii a zavedení do prevádzky by malo dôjsť k postupnej inštalácii uvedeného prístupového systému aj na pobočky monitorovacieho pracoviska.

Definovanie prístupových práv úzko súvisí s jednotlivými úlohami pracovísk, s definovaním účelu miestností, ale aj s definovaním pracovných pozícií v danej organizácii. Je nutné charakterizovať osoby, ktoré majú mať jednotlivé úrovne prístupu a je nevyhnutné zabezpečiť, aby do určitých priestorov nebolo možné vniknutie neoprávnenej osoby.

S prístupovým právom pre vstup je úzko spojené aj definovanie jednotlivých prístupových práv pre informačný systém, alebo manipuláciu s dokumentmi, ktoré zohrávajú úlohu nie len vo vedení firmy, ale aj vo vykonávaní určitej služby pre zákazníka.

Tab. 26. Návrh definovania priority pre zavedenie prístupového systému

Objekty riadenia	Určenie priority	Zdôvodnenie	Zodpovedná osoba	Termín
Olomouc	1	Najvyšší stupeň riadenia Oddelenie monitorovacieho pracoviska		Zahájenie pro.: Koniec pro.:
Praha	2	Najväčší počet zodpovedností za monitorovacie pracoviská		Zahájenie pro.: Koniec pro.:
Brno	3	Riadiace pracovisko so stupňom riadenia monitorovacích pracovísk		Zahájenie pro.: Koniec pro.:

ZDROJ: (autor)

Nasledujúca tabuľka definuje prístupové úrovne pre jednotlivé rozmiestnenie miestností, ale aj pre definované pracovné pozície, pričom nedochádza ku presnému stanoveniu jednotlivých pracovníkov. Základným definovaním je prístup do objektu.

Platia nasledujúce pravidlá:

- Každý zamestnanec má svoju prístupovú kartu,
- Karta je označená menom, funkciou a fotografiou,
- Zákazníci a klienti sa môžu v objekte pohybovať len v sprievode s oprávnenou osobou,
- Externí pracovníci sa taktiež v objekte môžu pohybovať len s oprávnenou osobou (priamym nadriadeným),
- Pracovníci, ktorí nemajú prístupové práva do vyhradených miestností sa v daných miestnostiach nemôžu zdržiavať,
- Vedenie spoločnosti má oprávnenie vstupovať do všetkých priestorov podniku.

Rizikové miestnosti spoločnosti, sú miestnosti, v ktorých je určitý pohyb osôb úplne zakázaný a je výlučne určené, ktoré osoby sa v daných priestoroch môžu pohybovať. Z hľadiska možnosti, že dôjde k poškodeniu materiálu medzi uvedené miestnosti patrí sklad materiálu, kancelárske priestory riaditeľa pobočky, ale hlavne aj vedenie obchodných

oddelení, a to z důvodu, že v danom priestore dochádza ku definovaniu zmluvných podmienok s klientom. Rizikovým priestorom je aj miestnosť pre výjazd hliadky a obsluhu. Do uvedených priestorov nesmú vstupovať osoby z externého prostredia. Jedná sa o zákazníkov a externých pracovníkov. Uvedený externí pracovníci majú povolený vstup iba v prípade školenia, kedy je do poručované naprogramovať voľný vstup do zasadacej miestnosti.

Každý pracovník musí súhlasiť s danými podmienkami a mal by byť s nimi dostatočne oboznámený, aby vedel v ktorých miestnostiach sa môže pohybovať. Hlavným cieľom je ochrániť zákazníka a jeho potreby, a to v uvedenom prípade, pretože spoločnosť je orientovaná na bezpečnosť, je nutné realizovať na zvýšenej úrovni.

Základné princípy prístupového systému:

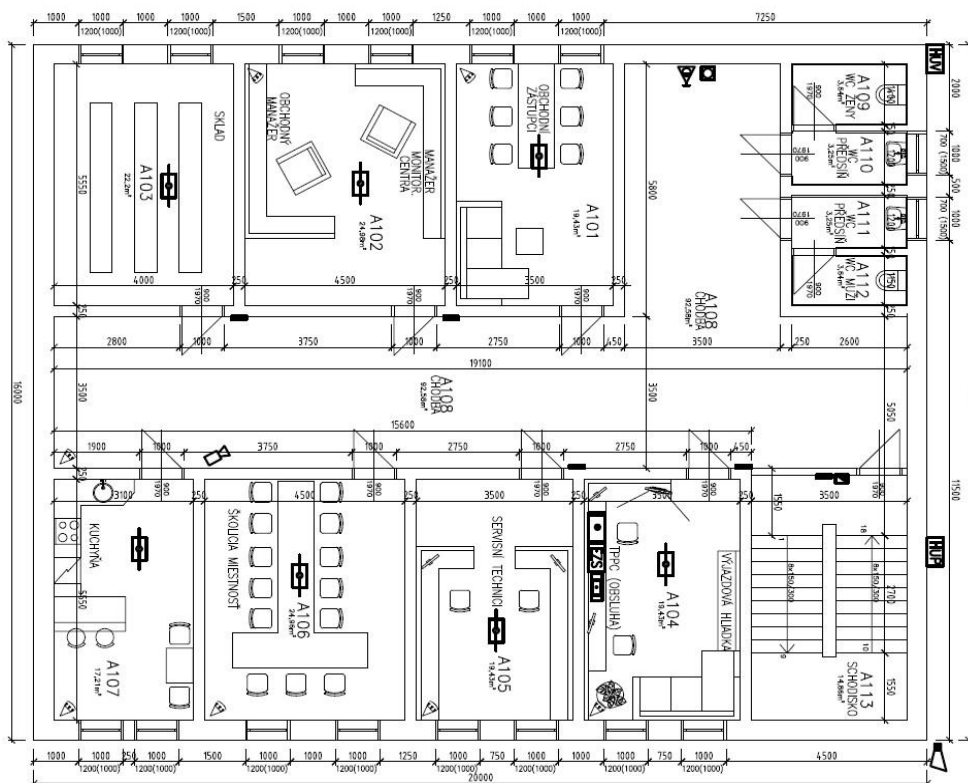
1. Prístupový systém musí spĺňať základné podmienky, ktoré sú určené uvedenou smernicou.
2. Každá zmena musí byť nahlásená zodpovednej osobe, ktorá je v každom objekte minimálne jedna.
3. Jednotlivé údaje o prístupoch sú vyhodnocované minimálne jeden krát za mesiac, kedy dochádza ku vyhodnoteniu prístupu zamestnancov do objektu, za cieľom výkazu o odpracovaných hodinách.
4. Každý zamestnanec musí byť preškolený o funkčnosti prístupového systému.
5. Externý zamestnanci majú zákaz pohybu v objekte riadenia mimo školiace miestnosti, a to len v termíne školenia a označenia, ako návštevy.
6. V prípade vchodu do objektu cudzej osoby, je nutné, aby danú osobu sprevádzal obchodný zástupca, v prípade klienta, ktorý chce vedieť, ako funguje firma, z dôvodu rozhodovania sa o zadaní zákazky, je nutné prehliadať objekt z manažérom monitorovacieho centra, zákazník nemá právo vstupovať do riadiacich miestností.
7. V prípade záujmu zákazníka o riadiace pobočky, je nutné udelenie výnimky z danej podmienky a to vedením formou zápisu a prehlásenia zákazníka.
8. Zamestnanec pri podpise zmluvy súhlasí so všeobecnými podmienkami podniku a organizácie.

5.4 Definovanie smernice pre členenie jednotlivých pracovísk

Členenie jednotlivých pracovísk je založené na rozdelení priestoru na miestnosti, jednotlivé miestnosti sú charakterizované určením cieľu, ktorý je naplňovaný jednotlivými funkciami v organizácii, ktoré zastávajú osoby, ktoré splňujú dané požiadavky na zamestnanca.

5.4.1 Definovanie smernice pre monitorovacie pracovisko

Monitorovacie pracoviská sa nachádzajú v jednotlivých mestách: Zlín, Jihlava, Ostrava, Ústí nad Labem, Liberec, České Budejovice, Pardubice, Hradec Králové. Každé uvedené mesto disponuje s uvedeným pracoviskom, ktoré sa nachádza vždy v podlaží budovy, čiže nie je na prízemí. Nasledujúci obrázok definuje navrhované rozmiestnenie jednotlivých kancelárskych priestorov. Uvedený obrázok je v plnom znení uvedený v prílohovej časti práce pod názov PRÍLOHA P I.



Obr. 49. Návrh rozmiestnenia monitorovacieho pracoviska pre jednotlivé mestá

ZDROJ: (autor)

Podľa funkcie monitorovacieho pracoviska, ktoré sú popísané vo vyššie uvedenej časti práci dochádza ku stanoveniu základných opatrení, ktoré by vzhľadom na danú vykonávanú

pracovnú oblasť mali byť splnené. Uvedený návrh je len orientačný a môže byť prispôsobený podľa stavebných dispozícií objektu, kde uvedená spoločnosť sídli, alebo prevádzkuje svoju činnosť.

Smernica pre definovanie požiadaviek pre monitorovacie pracoviská:

1. Každé monitorovacie pracovisko, by sa malo nachádzať v samostatnej budove, a v prípade, že uvedená podmienka nie je splniteľná, malo by uvedené pracovisko byť situované tak, aby sa jednotlivé kancelárske priestory nachádzali na spoločnom poschodí.
2. Uvedené samostatné poschodie by malo byť obsadené len uvedenou spoločnosťou, pričom by nemalo dochádzať k pohybu cudzích ľudí bez sprievodu.
3. Pred vstupom na poschodie by malo dochádzať ku oddeleniu od iných poschodí, čiže by sa nemalo daným poschodím prechádzať na iné poschodie a súčasne by mal byť vchod na poschodie zabezpečený pred vstupom neoprávnených osôb. (napríklad: sklenené dvere s prístupovým systémom)
4. V prípade, že sa jedná o poschodie budovy, ktorá má viacero poschodí, je nutné, aby schodisko, kde dochádza k pohybu neoprávnených osôb bolo oddelené od uvedeného pracoviska.
5. Každé monitorovacie pracovisko musí spĺňať podmienky uvedené vyššie v danom dokumente bezpečnostnej politiky, a to hlavne technické zabezpečenie daného pracoviska, ktoré taktiež môže byť navrhované s určitou odchýlkou tak, aby nedochádzalo k obmedzeniu jeho funkčnosti.

Odchýlky jednotlivých parametrov pre uvedené technické komponenty by mali byť stanovené pri konkrétnom návrhu jednotlivých pracovísk. Pričom by malo dochádzať k zhodnoteniu, či súčasné pracoviská odpovedajú požadovaným hodnotám, a naplňujú uvedené funkcie.

Tab. 27. Návrh finálneho hodnotenia splnenia požiadaviek určených smernicou

Pracovisko	Splňuje požiadavky na dané pracovisko určené smernicou bezpečnostnej politiky?		Je potrebný individuálny návrh rozmiestnia jednotlivých priestorov?		Je potrebné nájsť iné priestory na prevádzkovanie uvedeného pracoviska?	
	áno	nie	áno	nie	áno	nie
Zlín P1	áno	nie	áno	nie	áno	nie
Jihlava P2	áno	nie	áno	nie	áno	nie

ZDROJ: (autor)

Tabuľka číslo 28, reprezentuje finálne hodnotenie, ktorému predchádza hodnotenie podľa definovaných pravidiel uvedenými smernicami bezpečnostnej politiky. Daný dokument bude zhotovený, ako kontrolný zoznam, kde budú hodnotené splnené jednotlivé požiadavky na daný segment (napríklad: kamerové systémy, technické zabezpečenie, prístupový systém a iné).

Každá miestnosť disponuje charakteristickými informáciami, ktoré by mali byť rozdelené podľa dôvernosti vo vzťahu k organizácií a ku klientovi, rozdelenie informácií by malo byť upravené vnútornou normou.

Tab. 28. Návrh úpravy a kategorizácie manipulovaných informácií

Dokumentácia	Hodnotenie informácií			Kategorizácia		
	Veľmi tajné	Tajné	Dôverné	C Monitorovacie centrum	B Riadiaca pobočka 1/ 2	A Vedenie firmy
Zápisy z jednaní s klientom	•			•	kópia	
Zápisy o stave majetku klienta	•			•	kópia	
Protokoly o postupoch		•		•		dokumentácia
Projektové dokumentácie	•				•	dokumentácia
Pracovné výkazy			•		•	
Plánovacie dokumentácie		•			•	schvaľovanie
Výkazy o stave prevádzok	•			•	kópia	
Výkazy o stave servisu		•		•	kópia	
Výkazy o kontrole		•		•	kópia	
Reklamačné dokumenty			•	•	•	podľa zložitosti
Zmluvné podmienky medzi dodávateľmi		•			•	•
Doplnenie ďalších dokumentácií, podľa analytických procesov a doplňujúcich dokumentov.						

ZDROJ: (autor)

Uvedené hodnotenie by malo byť výsledkom zoskupenia každého dokumentu, ktorý sa v organizácií nachádza a podľa definovania jednotlivých informácií. Nezáleží len na danom dokumente, ale aj rozsahu klientovej zákazky, čiže dochádza síce k primárnej kategorizácií, ale je nutné pri hodnotení definovať aj dokumentáciu zvláštnu, ktorá vykazuje nasledujúce parametre.

Dokumentácia zvláštna:

- Dokumentácia obsahujúca závažné informácie, ktorých znehodnotením, alebo odcudzením by mohlo dôjsť k poškodeniu zákazníka.
- Dokumentácia, ktorá pojednáva o nadštandardnej zákazke, ktorá nespĺňa definované normy na kvantitu, alebo kvalitu predvídanej zákazky, ktoré sú definované, ako služby.
- Dokumentácia zákazníka, ktorý si vyslovene vyžiadal, aby uvedené dokumenty boli utajované a má k tomu iné, nie vždy známe dôvody.

Tab. 29. Návrh prístupových oprávnení pre vstup do miestností monitorovacieho pracoviska

	MIESTNOSŤ		sídlo	Povolený prístup	Dokumentácia			
					Definovanie	áno	nie	
Zlín, Jihlava, Ostrava, Ústí nad Labem, Liberec, České budějovice, Pardubice, Hradec králové	SKLAD	A 103	materiál	servisný technik	záznam o materiále			
				manažér monitorovacieho centra	záznam o výdaji			
				iné vedenie	záznam o prijíme materiálu			
					evidencia			
	OBCHODNÉ ODD.	kancelária A 102	Obchodný manažér	iné vedenie		nákup materiálu		
						záznam o klientoch		
			projekty					
			klientské zmluvy					
			definovanie podmienok					
	kancelária A 101	Obchodný zástupci		obchodný zástupci	obchodné stratégie			
				ZÁKAZNÍCI	plány			
				manažér monitorovacieho centra	definovanie podmienok			
				iné vedenie	sledovanie kontrol			
	Kuchyňa	A 107	každý z pobočky		definovanie materiálu a prevádzkových podmienok			
	Školiaca miestnosť	A106	každý z pobočky					
	Servisní technici	kancelária A 105	Servisný technik	servisný technik	kniha servisu			
technické vedenie				plánovanie inštalácií				
Servisný technik			iné vedenie	záznamy o zmene v systéme				
			manažér monitorovacieho centra	objednávkové dokumenty				
Tiesňové a poplachové prijímacie centrum	kancelária A 104	Výjazdová hliadka	manažér monitorovacieho centra	záznamy o výjazde				
			členovia výjazdovej hliadky	záznamy o kontrolach				
		Obsluha TPPC	obsluha TPPC	definovanie kontrol				
			obchodný manažér	informácie o klientoch				

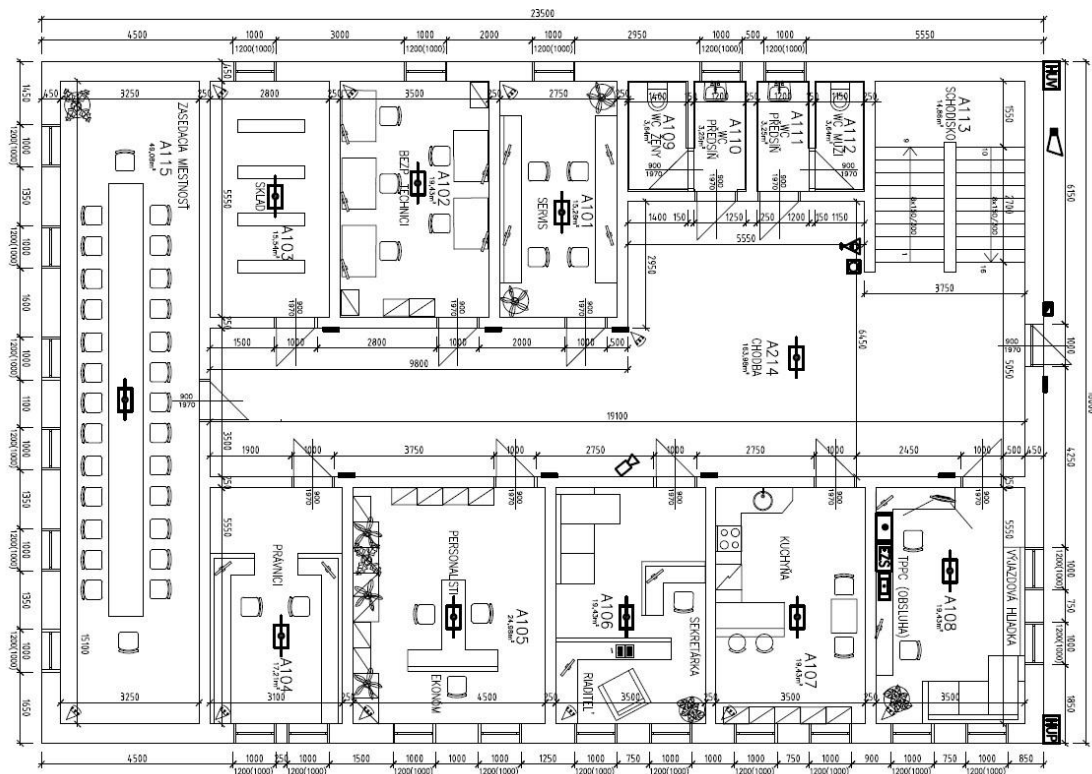
ZDROJ: (autor)

Monitorovacie pracovisko je pracovisko, kde dochádza ku primárnemu stupňu vedenia, a teda nachádza sa tu miestnosť prevádzkujúca monitoring zákazníkov, ale aj výjazdová hliadka. Výjazdová hliadka má primárne dve úlohy. Prvá je chrániť majetok organizácie, a teda zabezpečiť chod daného pracoviska, a to z pohľadu bezpečnosti v prípade, že pracovisko je v stave mimo prevádzky druhá, viac menej hlavná funkcia, ktorá vyplňuje

80% pracovnej náplne danej výjazdovej hliadky je zabezpečiť a strážiť majetok klienta. Na dané pracovné pozície sú popísané smernice pre výkon danej pozície a taktiež dochádza k určeniu smerníc pre neustále vzdelávanie výcvik.

5.4.2 Definovanie smernice pre riadiace pracovisko

Riadiace pracoviská danej organizácie sa nachádzajú v dvoch lokalizovaných prevádzkach, a to v Prahe a v Brne. Uvedené rozloženie ich funkcií je definované v sekcii definovanie vybranej organizácie. Každé z uvedených riadiacich pracovísk je charakteristické určitými priestorovými dispozíciami, ktoré je možné prispôbiť pre stanovenú bezpečnostnú politiku organizácie. Uvedený obrázok kancelárskeho sídla v Prahe je v plnom znení uvedený v prílohovej časti práce pod názov PRÍLOHA P II.

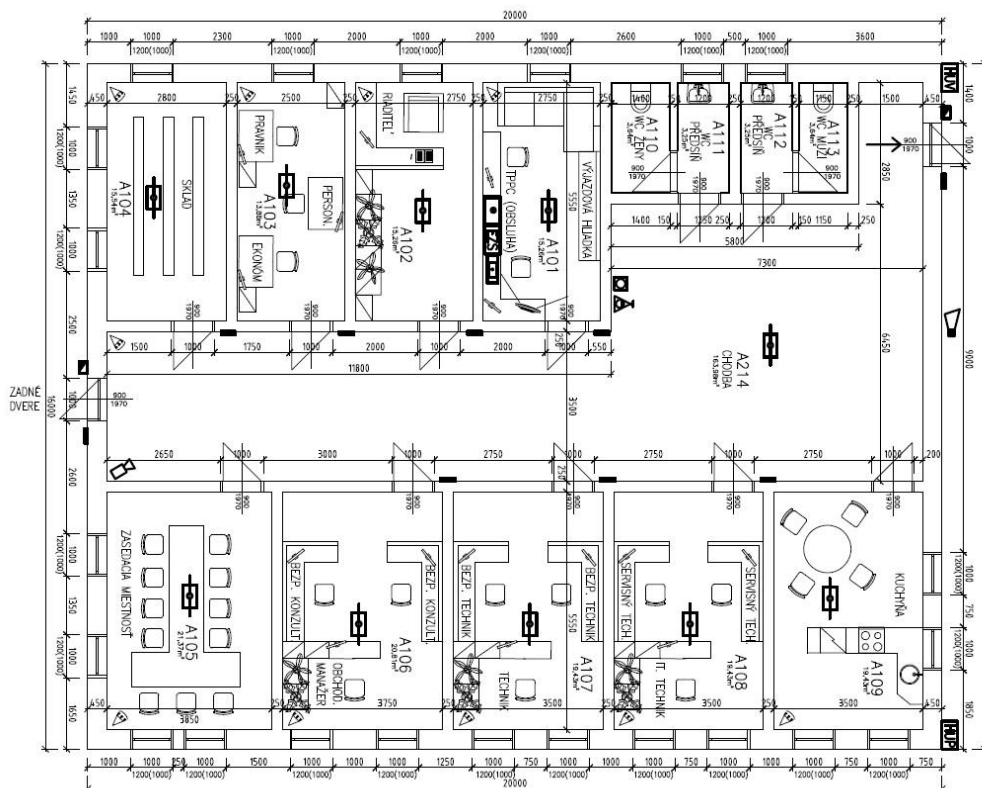


Obr. 50. Návrh rozmiestnenia riadiacej pobočky Praha

ZDROJ: (autor)

Uvedené riadiace pracovisko v Prahe nie je lokalizované na poschodí budovy, teda je na prízemí. V objekte sídli výlučne uvedená spoločnosť a schodisko vedie na druhé poschodie, ktoré je ale v súčasnej dobe nevyužitá a majitelia spoločnosti plánujú uvedené poschodie využiť pre funkcie spojené s plánovaným rozvojom spoločnosti. Uvedený obrázok

kancelárskeho sídla v Brne je v plnom znení uvedený v prílohovej časti práce pod názov PRÍLOHA P II.



Obr. 51. Návrh rozmiestnenia riadiacej pobočky Brno

ZDROJ: (autor)

Riadiaca pobočka v Brne je lokalizovaná v areáli kancelárskych budov, pričom samotná riadiaca pobočka sa nenachádza v kancelárskej budove, v ktorej sídli viacero firiem. Jedná sa o samostatnú budovu so samostatným vchodom, ale v hustej zástavbe, pričom v blízkom okolí sa nachádzajú iné objekty a vonkajší priestor nie je ohradený, ani zabezpečený proti vniknutiu do blízkeho prostredia budovy.

Smernica pre definovanie požiadaviek na riadiace pracoviská:

1. Každé riadiace pracovisko, ktoré disponuje súčasne s monitorovacím pracoviskom musí spĺňať požiadavky na prevádzku monitorovacieho pracoviska, ak na daný objekt nie sú definované prísnejšie kritériá. V tom prípade, musí dôjsť k naplneniu prísnejších kritérií.

2. Každé riadiace pracovisko by malo mať v okolí budovy definované parkovacie miesta, a to pre zamestnancov, zákazníkov, ale prioritne pre zásahovú hliadku.
3. Vstup do budovy riadiaceho pracoviska by mal byť chránený proti neoprávnenému vniknutiu cudzej osoby.
4. Okolie budovy by malo byť dostatočne chránené pred pohybom potenciálnych páchatel'ov.

Tab. 30. Návrh prístupových oprávnení pre vstup do miestností riadiacej pobočky

	MIESTNOSŤ		sídlo	Povolený prístup	Dokumentácia		
					Definovanie	áno	nie
Prah	SKLAD	A 103	materiál	Servisný technik	záznam o materiále		
				Manažér monitorovacieho centra	záznam o výdaji		
					záznam o prijíme materiálu		
				iné vedenie	evidencia		
	Technické oddelenie	kancelária A 102	Bezpečnostní technici	Manažér monitorovacieho centra	vedenie projektov		
				Projektanti	záznam o klientoch		
				Manažér technického oddelenia	záznamy o požiadavkách		
	SERVIS	A 101	Servisný technici	Technické vedenie	kniha servisu		
				iné vedenie	plánovanie inštalácií		
				Manažér monitorovacieho centra	záznamy o zmene v systéme		
				Iný servisní technici	objednávkové dokumenty		
	Právne oddelenie	kancelária A 104	právnicki	Manažér monitorovacieho centra	právne dokumenty		
				Iný právnicki	záväzky voči dodávateľom		
				Obchodný manažér	záväzky voči zákazníkom		
	Personálne oddelenie	A105	personalisti	Právnicki	požiadavky na zamestnancov		
				Personálne vedenie	testy a skúšobné dokumenty		
			ekonóm	Obchodný manažér			
				iné vedenie	ekonomické dokumenty		
	Kancelária riaditeľa	A106	riaditeľ	riaditeľ	záväzná dokumentácia		
			sekretárka		know how firmy		
Kuchyňa	A 107	každý z pobočky		definovanie materiálu a prevádzkových podmienok			
Školiaca miestnosť	A106	každý z pobočky					
Tiesňové a poplachové prijímacie centrum	kancelária A 108	Výjazdová hliadka	manažér monitorovacieho centra	záznamy o výjazde			
			členovia výjazdovej hliadky	záznamy o kontrolach			
		Obsluha TPPC	obsluha TPPC	definovanie kontrol			
			obchodný manažér	informácie o klientoch			

ZDROJ: (autor)

Návrh prístupových oprávnení súčasne definuje dokumentáciu, s ktorou dochádza k manipuláciám v rámci uvedenej lokalizácie pracoviska a jednotlivých kancelárií. Ak

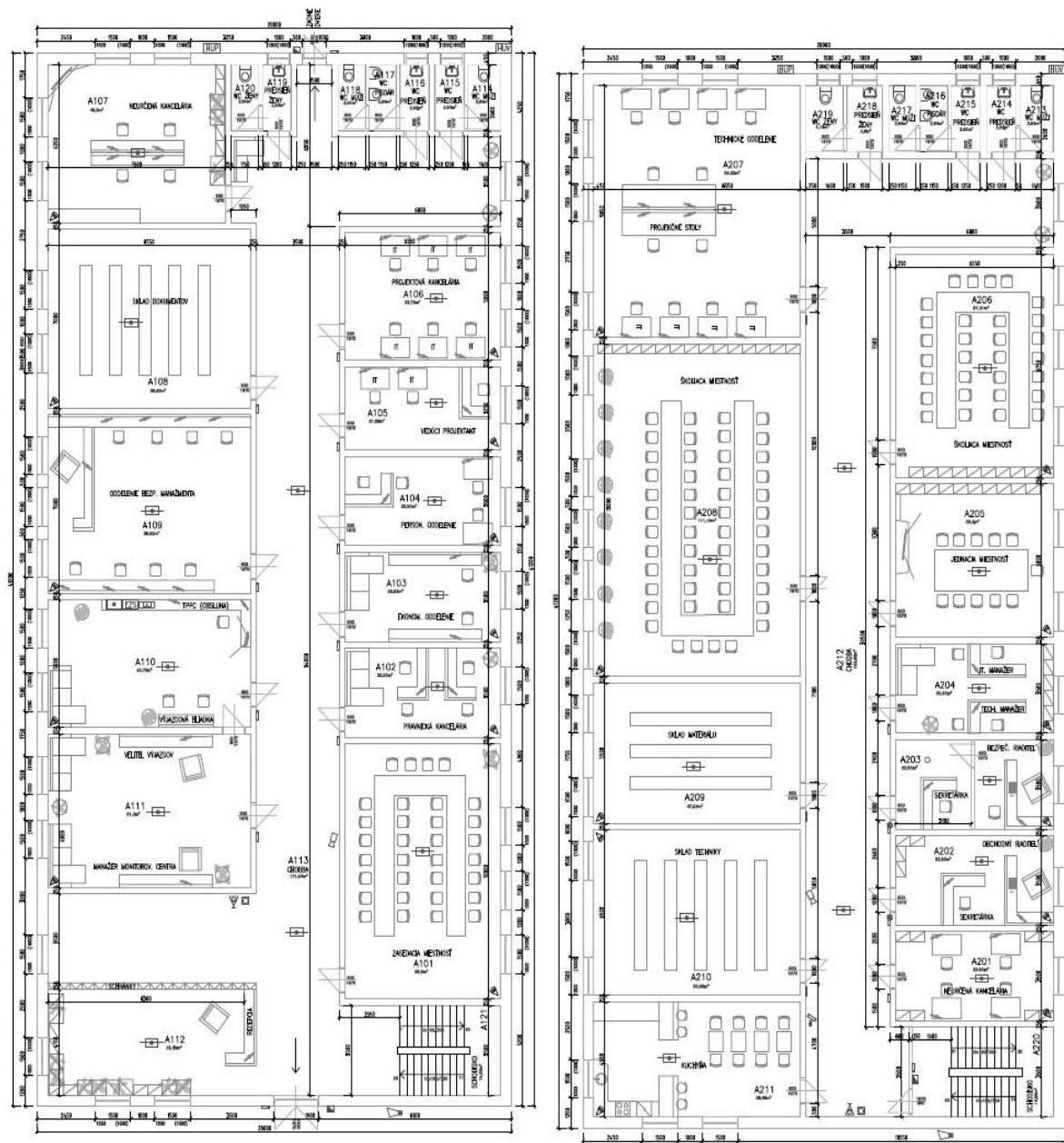
definujeme dokumentáciu, ktorá zaznamenáva informácie, je možné definovať pravidlá pre prístup, a to podľa charakteru informácií a ich hodnoty.

5.4.3 Definovanie smernice pre vedúce riadiace pracovisko Olomouc

Vedúce riadiace pracovisko v Olomouci je lokalizované v osobitnej kancelárskej budove. V budove nesídlí žiadna iná organizácia a je výlučne obývaná pracovníkmi spoločnosti. Budova sa nenachádza v areáli. Pre uvedenú prevádzku je nutné stanoviť smernicu, ktorá bude definovať najvyšší stupeň bezpečnosti vzhľadom k pobočkám spoločnosti, pretože v uvedenej budove dochádza k manipuláciám citlivých údajov.

Smernica pre definovanie požiadaviek na vedúce riadiace pracovisko:

1. Riadiace pracovisko musí byť lokalizované v samostatnej budove, a teda nesmie dochádzať k umiestneniu iných spoločností v budove.
2. Budova by mala mať vlastný areál, pričom by malo dochádzať k oploteniu vonkajšieho priestoru.
3. Vedúce riadiace pracovisko by malo byť situované do blízkosti plánovanej výstavby ďalších budov pre rozširovanie spoločnosti.
4. Následne by malo dochádzať k monitorovaniu a riadenému vstupu do areálu budovy.
5. V prízemí budovy vedúceho riadiaceho pracoviska by mala byť situovaná recepcia, ktorá monitoruje pohyb osôb v danom objekte, a zároveň riadi a plánuje jednotlivé zvolávané akcie.
6. V budúcom vývoji spoločnosti je nutné, aby pred vstupom do areálu spoločnosti bola taktiež služba zaisťujúca pohyb automobilov, ale aj vynášanie a donášanie predmetov do objektu.
7. V prípade výstavby a zahájenia činnosti rozširovania spoločnosti je nutné klasifikovať dokumentáciu spojenú s výstavbou, ale aj so samotnou prevádzkou daných objektov.



Obr. 52. Návrh pre rozmiestnenie vedúceho riadiaceho pracoviska Olomouc (vľavo: 1PP, vpravo: 1NP)

ZDROJ: (autor)

Uvedený obrázok definovania vedúceho riadiaceho pracoviska je v plnom znení uvedený v prílohovej časti práce pod názov PRÍLOHA P IV a PRÍLOHA PV. Vedúce riadiace pracovisko riadi a koordinuje celú činnosť organizácie. Dochádza k sústredeniu pracovníkov, ktorí sa podieľajú na jednotlivých projektoch, pričom dochádzajú ku styku s veľmi dôležitými informáciami z pobočiek, ktoré im prislúchajú na dané vedenie, alebo návrh projektu.

Tab. 31. Návrh prístupových oprávnení pre vstup do miestností vedúcej riadiacej pobočky
Olomouc prízemie

MIESTNOSŤ	sídlo	Povolený prístup	Dokumentácia				
			Definovanie	áno	nie		
<i>Prízemie</i>							
Recepcia	A112	monitoring	každý	záznamy o prístupe do objektu			
Manažment tiesňového a poplachového prijímacieho centra	A 111	Manažér monitorovacieho centra	Vedenie spoločnosti	záznamy o poplachoch			
				záznamy o stave prevádzok klientov			
		Veliteľ výjazdovej hliadky		záznamy o kontrolách			
				dokumenty o stave podniku			
Tiesňové a poplachové prijímacie centrum	kancelária A 110	Výjazdová hliadka	Manažér monitorovacieho centra	záznamy o výjazde			
			členovia výjazdovej hliadky	záznamy o kontrolách			
		Obsluha TPPC	obsluha TPPC	definovanie kontrol			
			obchodný manažér	informácie o klientoch			
Oddelenie bezpečnostného manažmentu	kancelária A 109	Bezpečnostní konzultant	Manažér monitorovacieho centra	bezpečnostné smernice			
			Vedúci audítor	Bezpečnostný technik	smernice pre výkon funkcií		
		Interný audítor	obchodný manažér	dokumenty definujúce prácu externých zamestnancov			
			iné vedenie	dokumenty o manažmentu organizácie			
		Servisní technici	Technické vedenie		knihy servisu		
					plánovanie inštalácií		
				Iný servisní technici	záznamy o zmene v systéme		
SKLAD dokumentov	A 108	dokumentácie	vedenie spoločnosti	záznamy o klientoch			
				záznam o výdaji			
				záznamy o inštaláciách a servise			
				evidencia			
neurčená kancelária	A 107	Voľné priestory (možnosť jednanja zo zákazníkmi)					
Projektová kancelária	A 106	projektanti	Technické vedenie	technické dokumentácie			
			obchodný manažér	projekčné dokumenty			
			Manažér monitorovacieho centra	IT návrhy			
Kancelária vedúci projektant	A 105	Vedúci projektant	Vedenie spoločnosti	kompletné projekty			
Personálne oddelenie	A 104	personalisti	Právnicki	požiadavky na zamestnancov			
			Personálne vedenie	testy a skúšobné dokumenty			
			Obchodný manažér				
Ekonomické oddelenie	A 103	ekonómovia	iné vedenie	ekonomické dokumenty			
			Manažér monitorovacieho centra	dokumenty o stave podniku			
Právne oddelenie	kancelária A 102	právnicki	Manažér monitorovacieho centra	právne dokumenty			
			Iný právnicki	záväzky voči dodávateľom			
			Obchodný manažér	záväzky voči zákazníkmi			
Zasadacia miestnosť	A 101	32 osôb	každý vopred nahlásiť	definovanie materiálu a prevádzkových podmienok			

ZDROJ: (autor)

Tab. 32. Návrh prístupových oprávnení pre vstup do miestností vedúcej riadiacej pobočky
Olomouc I. poschodie

MIESTNOSŤ	sídlo	Povolený prístup	Dokumentácia		
			Definovanie	áno	nie
<i>1. poschodie</i>					
Kuchyňa	A 211	každý z pobočky	definovanie materiálu a prevádzkových podmienok		
SKLAD techniky	A 210	technika	Servisný technik	záznam o technike	
			Manažér monitorovacieho centra	záznam o výdaji záznam o prijme technických komponentov	
			iné vedenie	evidencia	
SKLAD	A 209	materiál	Servisný technik	záznam o materiáli	
			Manažér monitorovacieho centra	záznam o výdaji záznam o prijme materiálu	
			iné vedenie	evidencia	
Školiaca miestnosť	A 208	50 osôb	každý vopred nahlásiť	definovanie materiálu a prevádzkových podmienok	
Technické oddelenie	kancelária A 207	Bezpečnostní technici	Manažér monitorovacieho centra	vedenie projektov	
			Projektanti	záznam o klientoch	
			Manažér technického oddelenia	záznamy o požiadavkách	
Školiaca miestnosť	A 206	30 osôb	každý vopred nahlásiť	definovanie materiálu a prevádzkových podmienok	
Jednacia miestnosť	A 205	11 osôb	každý vopred nahlásiť	definovanie materiálu a prevádzkových podmienok	
Technický manažment	A 204	Technický manažér	Manažér monitorovacieho	technické dokumentácii	
		IT manažér	iné vedenie	IT projekty informačných systémov	
Bezpečnostný riaditeľ	A 203	riaditeľ	riaditeľ	záväzná dokumentácia	
		sekretárka		know how firmy	
Obchodný riaditeľ	A 202	riaditeľ	riaditeľ	záväzná dokumentácia	
		sekretárka		know how firmy	
neurčená kancelária	A 201	Vofné priestory (možnosť jednania zo zákaznikom)			

ZDROJ: (autor)

Tabuľka číslo 32 a tabuľka číslo 33 definuje jednotlivé kancelárske priestory a ich rozloženie, pričom následne dochádza ku stanoveniu dokumentácie, s ktorou sa v daných kancelárskych priestoroch manipuluje a súčasne sú definované prístupy do jednotlivých kancelárskych priestorov. V prípade, že sa jedná o vstup do danej jednotky osobou, ktorá nemá povolený prístup, je daný vstup možný realizovať len v doprovide s oprávnenou osobou. Na základe uvedenej skutočnosti je nutné uvedený fakt zakomponovať do smernice pod číslom 8 a číslom 9.

8. V prípade potreby vstupu neoprávnenej osoby do kancelárskych priestorov, ktoré nemajú danú osobu definovanú ako osobu povolenú, je vstup možný iba za prítomnosti osoby, ktorá má daný vstup povolený a v prípade kontroly musí byť prítomnosť tretej osoby odôvodnená.
9. V prípade, že sa jedná o vstup do kancelárií vedenia spoločnosti (kancelária riaditeľa, manažéra a iné), je možný vstup tretej osoby len za sprievodu osoby, ktorá

v danej kancelárii sídli. (neplatí pre neohlasované kontroly, kedy daný pracovník nesmie byť prítomný v kancelárii, aby neovplyvnil priebeh kontroly)

5.5 Definovanie smernice pre určenie požiadaviek na zamestnancov

Nasledujúca navrhovaná smernica definuje požiadavky na kvalifikáciu a prax jednotlivých pracovných pozícií. Definovanie pracovných pozícií je jedným zo základných požiadaviek pre správny výkon organizácie, a tým poskytnutie adekvátnych a kvalitných služieb. Pod požiadavkami na zamestnancov sa rozumie taktiež definovanie školiacich procesov a rekvalifikácií na určitý druh práce.

Tab. 33. Definovanie primárnych dokumentov pre určenie požiadaviek na zamestnancov

Oddelenie	Dokumentácia						
Obchodné oddelenie	Smernica pre kvalifikačné požiadavky a prax	Požiadavky na osobnostné predpoklady pre výkon pracovnej pozície	Smernica pre certifikácie a rekvalifikácie v danom obore	Plánovanie školení z uvedeného oboru práce	Smernica pre školenia BOZP	Smernica pre iné bezpečnostné školenia	Plánovanie školení v oblasti bezpečnosti a zavádzania nových metód
Oddelenie bezpečnostného manažmentu	Smernica pre splnenie zákonom stanovených podmienok na certifikovanú osobu		Smernica pre kvalifikačné požiadavky a prax	Smernica pre certifikácie a rekvalifikácie v danom obore	Plánovanie školení z uvedeného oboru práce pre zvyšovanie kvalifikácie		Smernica pre školenia BOZP
	Smernica pre definovanie chovania sa v krízových situáciách		Smernica pre definovanie pracovnej náplne		Definovanie postihov v prípade neplnenia uvedených požiadaviek na danú pracovnú pozíciu		
Personálne oddelenie	Smernica pre kvalifikačné požiadavky a prax	Požiadavky na osobnostné predpoklady pre výkon pracovnej pozície	Plánovanie školení z uvedeného oboru práce	Smernica pre školenia BOZP	Smernica pre iné bezpečnostné školenia	Plánovanie školení v oblasti bezpečnosti a zavádzania nových metód	
IT oddelenie	Smernica pre splnenie zákonom stanovených podmienok na certifikovanú osobu		Smernica pre kvalifikačné požiadavky a prax	Smernica pre certifikácie a rekvalifikácie v danom obore	Plánovanie školení z uvedeného oboru práce pre zvyšovanie kvalifikácie		Smernica pre školenia BOZP
Právnické oddelenie	Smernica pre kvalifikačné požiadavky a prax	Smernica pre školenia BOZP	Plánovanie školení z uvedeného oboru práce	Smernica pre iné bezpečnostné školenia	Plánovanie školení v oblasti bezpečnosti a zavádzania nových metód		Plánovanie školení z nových strategických plánov
Ekonomické oddelenie	Smernica pre kvalifikačné požiadavky a prax	Smernica pre školenia BOZP	Plánovanie školení z uvedeného oboru práce	Smernica pre iné bezpečnostné školenia	Plánovanie školení v oblasti bezpečnosti a zavádzania nových metód		Plánovanie školení z nových strategických plánov

ZDROJ: (autor)

V nasledujúcej časti práce dochádza ku definovaniu základnej smernice pre vytvorenie celkovej dokumentácie a požiadaviek pre technické a obchodné pracovné pozície.

5.5.1 Smernica pre technické pracovné pozície

Smernica pre technické pracovné pozície stanovuje primárnu požiadavku, a to splňovať podmienky stanovené zákonom, a to konkrétne vyhláškou číslo 50/1978 Sb., ktorá definuje požiadavky na kvalifikáciu v obore elektrotechniky a projektovania.

Technické pracovné pozície:

- Manažér technického oddelenia,
- Manažér monitorovacieho pracoviska,
- Vedúci projektant,
- Projektant,
- Servisný technik,
- Bezpečnostný technik,
- Bezpečnostný konzultant,
- Manažér IT,
- Technik IT.

Tab. 34. Návrh tabuľkového zhodnotenia jednotlivých pracovných požiadaviek

Pozícia	Meno	Vzdelanie	Prax	Certifikácie	Plánované rekvifikácie	
					Názov	Dátum

ZDROJ: (autor)

Návrh smernice pre technické pracovné pozície:

1. Každá pracovná pozícia musí mať definovanú kartu pracovnej pozície, ktorá sa skladá z troch častí, a to požiadavky na prax a kvalifikáciu, popis pracovnej činnosti a plán rekvifikácií.
2. Technické pracovné pozície musia spĺňať požiadavky určené zákonom. (elektrotechnika)
3. Každá technická pracovná pozícia musí byť pravidelne preškoľovaná v oblasti bezpečnosti práce a v oblasti požiarnej ochrany.
4. Každý bezpečnostný technik sa musí pravidelne zúčastňovať na školeniach, ktoré organizuje dodávateľská spoločnosť.
5. Požiadavky na technické pozície sú pravidelne preverované a k ich prevereniu dochádza v dvoch častiach, a to ku plánovaným previerkam, ktoré sú s časovým

predstihom oznámené a ku neplánovaným previerkam, ktoré oznamované nie sú, ale uvedený pracovník s ich vykonaním súhlasí dňom podpisu pracovnej zmluvy, v ktorej je uvedený fakt definovaný.

6. Rekvalifikačné dokumenty musí uvedený pracovník vždy odovzdať na príslušnom personálnom oddelení. Ak došlo ku hradeniu čiastky rekvalifikačného kurzu spoločnosťou, má daná spoločnosť nárok na originál osvedčenia a uvedená osoba na kópiu. Ak si uvedená osoba hradila daný kurz sama, spoločnosť má nárok na kópiu uvedeného osvedčenia, a to za účelom zvýšenia kvalifikácie.

K ďalšiemu definovaniu požiadaviek na uvedené pracovné pozície dochádza po definovaní a skompletizovaní uvedených dokumentov.

5.5.2 Smernica pre obchodné pracovné pozície

Obchodné pracovné pozície sú pozície, ktoré vzhľadom na povahu uvedenej organizácie najviac pôsobia na jej vývoj spolu s technickými pracovnými pozíciami, a to hlavne z dôvodu, že primárna potreba je uspokojiť potrebu zákazníka, k čomu dochádza pomocou technického zabezpečenia a sprostredkovania obchodu.

Obchodné pracovné pozície:

- Obchodný manažér,
- Manažér monitorovacieho centra,
- Vedúci audítor,
- Interný audítor,
- Obchodný zástupca,
- Bezpečnostný konzultant.

Pracovné pozície bezpečnostný konzultant a manažér monitorovacieho centra sú pozície obchodne technické, a to z dôvodu, že je nevyhnutné, aby dané osoby boli technicky zdatné, ale zároveň, aby ovládali obchodné praktiky a plány spoločnosti. Jednotlivé obchodné pozície musia ovládať prácu s informáciami, a to za cieľom, aby nedochádzalo k úniku interných informácií, ale mali by ovládať aj postupy na získanie zákazníka a z uvedeného dôvodu sa jedná primárne o nasledujúce interné školenia pre obchodné pozície.

Definovanie školení v oblasti:

- Obchodné znalosti a znalosti vyjednávania,
- Školenie služieb ponúkaných zákazníkom,
- Školenie technických špecifikácií pre obchodníkov,
- Certifikácie ISO noriem,
- Školenie pre prácu s informačnými systémami,
- Školenie pre prácu s informáciami,
- Školenie proti sociálnemu inžinierstvu.

Uvedené návrhy pre školenia sú len orientačné a mali by byť pravidelne doplňované podľa požiadaviek osôb zodpovedných za vedenie uvedených pracovných pozícií.

Návrh smernice pre obchodné pozície:

1. Každý obchodný pracovník musí byť pravidelne preškolený pre prácu s informáciami, aby nedochádzalo k úniku citlivých údajov.
2. Každý obchodný pracovník musí byť pravidelne preškolený v oblasti vplyvu sociálneho inžinierstva.
3. Každý obchodný pracovník by mal ovládať prácu v Informačnom systéme spoločnosti.
4. Obchodný zástupca nesmie komunikovať s potenciálnym zákazníkom o internom procese firmy.
5. Obchodný zástupca musí pravidelne zaznamenať údaje, ktoré zákazníkovi poskytol.
6. Obchodný zástupca je viazaný mlčanlivosťou ohľadne informácií získaných od klienta, a to vo vzťahu k cudzej tretej osobe.
7. Audítor spoločnosti nesmie vynášať informácie o spoločnosti mimo danú spoločnosť. Jeho dokumentácie je prístupná len pre vedenie spoločnosti, a to v dopredu určených kompetenciách.
8. Každá obchodná schôdzka musí byť dokumentovaná a v určitom intervale zaznamenaná do plánovacieho kalendára, ktorý schvaľuje zodpovedná osoba, vždy priamy nadriadený.

9. V prípade, že dôjde k porušeniu určených požiadaviek musia byť definované sankcie. V prípade poškodenia mena spoločnosti dochádza k okamžitému rozviazaniu pracovnej zmluvy a vynucovaniu ďalších zmluvne určených sankcií.

Uvedená smernica je následne rozširovaná o ďalšie požiadavky, ktoré vyplývajú z dokumentov, ktoré majú byť spracované v určitom časovom intervale od ich naplánovania. V prípade, že je smernica kompletná dochádza k oboznámeniu zamestnancov s uvedenou smernicou, a následne dochádza ku aplikovaniu do praxe.

5.6 Definovanie smernice pre ochranu života a zdravia osôb

Smernica pre ochranu života a zdravia osôb na pracovisku danej organizácie je interný predpis, ktorý je všeobecne platný pre každého zamestnanca spoločnosti, a to bez ohľadu na stupeň riadenia a výkon funkcie. Podľa funkčného zaradenia dochádza k určeniu miery zodpovednosti za určené oblasti, ktorých sa ochrana dotýka. Vedenie spoločnosti musí vymenovať zodpovedné osoby, ktoré prevádzajú a zabezpečujú určité stupne školenia, pričom uvedené vymenovanie musí mať vždy písomnú formu. Vedenie spoločnosti má taktiež v kompetencií určenie pracovníkov, ktorý sa zúčastnia školenia vedúcich pracovníkov z oboru zásad bezpečnosti práce a ochrany zdravia pri práci.

Návrh smernice pre bezpečnosť a ochranu zdravia pri práci:

1. Každý zamestnanec spoločnosti je povinný sa pravidelne zúčastňovať predpísaného školenia v oblasti bezpečnosti a ochrany zdravia pri práci, a to ako súčasť svojej kvalifikácie.
2. Vedenie spoločnosti musí písomne vymenovať osoby, ktoré sú zodpovedné za uvedené úlohy, pričom v menovacom dekrete musia byť definované procesy, za ktoré daná osoba zodpovedá, ale aj sankcie, ktoré za porušenie hrozia a samozrejme kompetencie v danom obore. Funkcia v oblasti BOZP je doplnková ku danej funkcií uvedenej osoby v spoločnosti, a musí dôjsť k verejnému menovaniu osoby podľa funkcie zastávajúcej procesy v oblasti BOZP.

Tab. 35. Návrh pre definovanie zodpovedných osôb z oblasti BOZP

FUNKCIA BOZP	Meno a priezvisko danej osoby	Úlohy pre výkon funkcie vo vzťahu k BOZP	Dokument menovania a dátum
DOHLAD BOZP Jednatel' spoločnosti (Obchodný riaditeľ, Bezpečnostný riaditeľ, Riaditeľ pobočky Brno, Riaditeľ pobočky Praha)	Ing. Peter Dočkalský (Ing. Jarmila Chovanová, Ing. Libor Gajdoš, Mgr. Vlastimil Pokorný, Mgr. Ondrej Krátky)	Zaistiť, aby každý prijatý zamestnanec pred nástupom do zamestnania absolvoval vstupné školenie (VNÚTORNÁ SMERNICA)	
VEREJNE ZODPOVEDNÁ OSOBA V OBLASTI BOZP (Personálny manažér, Veliteľ výjazdovej hliadky Manažér technického oddelenia, Manažér monitorovacieho centra)	Petra Dubáková Luboš Vlk Tomáš Drozd Zlín: Ingrid Lubovská Jihlava: Bc. Aneta Janotová Ostrava: Mária Kordíaková Olomouc: Ing. Lucia Dubová Liberec: Miloš Jarina Ú. n. Labem: Karol Mázik Č. Budejovice: Kamila Nováková Pardubice: Martina Veselá Hr. Králové: Jana Švehlová	Zodpovedá za pravidelné školenia v oblasti BOZP u podriadených zamestnancov Zodpovedá za preverovanie a preskúšanie z predpisov BOZP a pokynov BOZP u podriadených zamestnancov Zodpovedá za vstupné školenia pre nových zamestnancov Zodpovedá za plnenie plánov pre opakované školenia v oblasti BOZP, a to v stanovených lehotách	
Odborne spôsobilá osoba v oblasti prevencii rizík BOZP Bezpečnostný technik	Olomouc: Petr Bochnat Brno: Karol Donský Praha: Petr Soukup	Zodpovedá za riadenie procesu školenia zamestnancov zo zásad BOZP v rámci celej organizácie Zodpovedá za spracovanie vnútorných predpisov pre školenia a realizáciu zo zásad BOZP, aktualizuje osnovy a navrhuje zmeny Zodpovedá za dokumentáciu skúšok z prevádzaných školení a riadi ukladanie záznamov Zodpovedá za aktuálne plány školení BOZP a ich osnovy	

ZDROJ: (autor)

Podľa zákonníka práce č. 262/2006 Sb. dochádza ku definovaniu interných požiadaviek, ktoré definujú, čo musí firma (zamestnávateľ) vykonať v oblasti školenia zásad BOZP, jedná sa o zakotvenie právnych požiadaviek do internej smernice.

- Každý zamestnanec musí byť pred samotným výkonom práce oboznámený s pracovným poriadkom a s právnymi dokumentmi, ktoré sa vzťahujú k oblasti bezpečnosti a ochrany zdravia pri práci, a taktiež musí byť oboznámený s kolektívnou zmluvou a vnútornými predpismi, ktoré okrem iného definujú hlavné zodpovedné osoby.
- Uvedené informácie musia byť vždy poskytnuté zamestnancovi v prípade, že sa jedná o prijatie do zamestnania, o jeho prevedenie, alebo preloženie na inú vykonávanú funkciu, alebo zmene pracovnej náplne, alebo zmene pracovného

prostredia, ktorá je spôsobená zavedením nových technických prístrojov, prostriedkov, alebo technológií. O uvedenom oboznamovaní zamestnancov je nevyhnutné viesť dokumentáciu, ktorú má v kompetencií odborne spôsobilá osoba v oblasti BOZP, menovaná jednatelom spoločnosti.

5. Zamestnanci musia byť pravidelne oboznamovaný s rizikami, výsledkami hodnotenia rizík, ktoré pri danej práci hrozia a s opatreniami, ktoré sú implementované do procesu za účelom ochrany pred definovanými rizikami.
6. V prípade, že dochádza k vykonávaniu pracovnej činnosti externého pracovníka, alebo zamestnanca inej spoločnosti, je nutné definovať zodpovednú osobu, ktorá zabezpečí, že externý pracovník bude informovaný a oboznámený s pokynmi pre zaistenie bezpečnosti a ochrany zdravia pri práci, a to primárne ku opatreniam zdolania požiaru, poskytnutia prvej pomoci a evakuácie fyzických osôb v prípade mimoriadnej udalosti. (Verejne zodpovedná osoba v oblasti BOZP)

V uvedenom prípade je spisovaný dokument, ktorý definuje činnosť tretej strany v organizácií, kde dochádza k hodnoteniu nevyhnutnosti povolania cudzej osoby do procesu firmy. Dochádza k schvaľovaniu na porade vedenia, kde následne po schválení privolania danej tretej osoby, dochádza k definovaniu podmienok, za ktorých danú pracovnú náplň vykoná.

7. Zamestnanci musia byť pravidelne preškoľovaný v oblasti právnych predpisov a iných predpisov, ktoré zabezpečujú bezpečnosť a ochranu osôb pri vykonávaní danej pracovnej náplne.
8. Zamestnanci musia byť pravidelne kontrolovaný v oblasti dodržiavania podmienok, na ktoré boli v uvedenej oblasti preškoľovaný. Kontrola môže byť realizovaná bez ohlásenia kontroly s predstihom.
9. Školenie musí byť prevedené v nasledujúcich prípadoch.

Tab. 36. Definovanie prípadu školenia v oblasti BOZP

Nástup zamestnanca do práce
Pri zmene pracovného zaradenia
Pri zmene druhu práce
Pri zavedení novej technológie, alebo zmeny výrobných a pracovných prostriedkov
Pri zmene pracovných postupov a technologických postupov
V iných prípadoch ktoré môžu mať podstatný vplyv na bezpečnosť a ochranu zdravia pri práci
V prípade vykonania určitej funkcie externým pracovníkom, alebo pracovníkom inej spoločnosti

ZDROJ: (autor)

10. V prípade, že závažnosť rizika a jeho povaha vyžaduje, aby dané školenie bolo pravidelne opakované, dochádza k určeniu intervalu opakovanosti a naplánovaniu daného školiaceho termínu. Ak povaha rizika vyžaduje okamžité prevedenie školenia, je školenie bez odkladu realizované v potrebnej miere, a to s určením priority.

Bezpečnostný technik spolu s verejne zodpovednými osobami za BOZP sa pravidelne stretávajú na taktickej porade vedenia opatrení pre aktuálnosť požiadaviek BOZP, kde dochádza k návrhu úprav a definovaniu potrebnej dokumentácie, poprípade dochádza k riešeniu problémových vyhodnotení, alebo situácií.

Tab. 37. Definovanie základnej osnovy v oblasti jednanie taktickej porady BOZP

ŠKOLENIE	Obsah školenia	Spôsob overenia znalostí	Spôsob kontroly dodržiavania v praxi	Plánovaný termín kontroly	Stav po kontrole	Dokumentácia

ZDROJ: (autor)

Nasledujúca tabuľka definuje systém školenia, ktorý má za účel zaistiť informovanosť zamestnancov v oblasti BOZP. Jedná sa o realizáciu výchovy vzdelávania v oblasti BOZP.

Tab. 38. Definovanie systému školiaceho procesu

Druh školenia	Popis školenia	Zodpovedná osoba
Vstupné školenie	<ul style="list-style-type: none"> • Informácie o politike firmy • Bezpečnostné pravidlá • Systém kvality a riadenia • Životné prostredie a environmentalistika • Systém pravidiel komunikácie • Systém pracovnej náplne 	Personálny zástupca Priamy nadriadený uvedeného zamestnanca
Vstupné školenie BOZP	<ul style="list-style-type: none"> • Osnova školenia schválená pre danú pracovnú funkciu • Oboznámenie s periodicitou školení • Oboznámenie s určením zamestnancov a zodpovedností • Oboznámenie o dôvode školení • Definovanie rizík hroziacich pri uvedenej práci a ich hodnotenie • Definovanie právnych predpisov vzhľadom k BOZP • Návody pre obsluhu strojov a iných zariadení potrebných pre prácu 	Bezpečnostný technik Priamy nadriadený zamestnanca
Praktický zácvik na pracovisku	<ul style="list-style-type: none"> • Definovanie presnej pracovnej náplne zamestnanca • Teoretické a praktické overenie zručností zamestnanca na výkon danej funkcie • Nutné písomný zápis 	Priamy nadriadený zamestnanca
Periodické školenie BOZP	<ul style="list-style-type: none"> • Oboznámenie so zmenami v oblasti BOZP • Oboznámenie s novými procesmi vo firme, ktoré vyžadujú nové pravidlá v oblasti BOZP 	Bezpečnostný technik Priamy nadriadený zamestnanca

	<ul style="list-style-type: none"> Interval minimálne 1 -2 krát za rok Prevádzka sa podľa osnovy stanovenej menovanými osobami 	
Vstupné a periodické školenie pre vybrané pracovné pozície	<ul style="list-style-type: none"> Školenie je zabezpečené externou firmou, ktorá disponuje s odbornou spôsobilosťou na daný výkon školenia Vybrané pracovné pozície sú určené vedením spoločnosti, a to v karte uvedenej pracovnej pozícií 	<p>Personálny zástupca Bezpečnostný technik Priamy nadriadený zamestnanca</p>
Mimoriadne školenia o BOZP	<ul style="list-style-type: none"> Dochádza k ich zvolávaniu v prípade mimoriadnej udalosti Za mimoriadnu udalosť sa v uvedenom prípade pokladá: <ol style="list-style-type: none"> zmena technológie zmena postupu výkonu práce zmena bezpečnostného predpisu zavedenie nového pracovného nástroja v prípade smrteľného pracovného úrazu v prípade zvýšenia rizika vzniku nepriaznivej udalosti v prípade obmedzenia výkonu pracovných pozícií z dôvodu rekonštrukcie, alebo iné. 	<p>Bezpečnostný riaditeľ Riaditeľ pobočky Bezpečnostný technik Manažér monitorovacieho centra</p>
Poučenie o pracovnom úraze	<ul style="list-style-type: none"> Definovanie zdroja a príčin pracovného úrazu, ktorý vznikol Nápravné riešenie, aby k danému pracovnému úrazu nedochádzalo Poučenie zamestnanca o nápravnom riešení, v prípade, že sa jedná o odhalenie novej hrozby poučenie všetkých dotknutých zamestnancov 	
Vstupné školenie nových vedúcich zamestnancov	<ul style="list-style-type: none"> Definovanie možných rizík pri práci, nielen pri práci pri výkone danej vedúcej pracovnej pozície, ale aj o rizikách, ktoré hrozia podriadeným zamestnancom vedúceho zamestnanca Predpisy a pokyny pre bezpečnosť a ochranu zdravia pri práci pre celé oddelenie Návody k postupom a definovanie kompetencií v určitých typizovaných udalostiach Certifikácia a zaznamenané skúšky v určených intervaloch 	<p>Bezpečnostný riaditeľ Bezpečnostný technik</p>
Periodické školenie vedúcich zamestnancov	<ul style="list-style-type: none"> Realizované za cieľom oboznámenia vedúcich zamestnancov o zmene v bezpečnostných predpisoch Definovanie nových bezpečnostných pravidiel Zhodnotenie predchádzajúcich nehôd Návrhy na zlepšenie Vplyv na faktory zapríčínujúce vznik nehody Vyhodnotenie meraných analýz 	<p>Bezpečnostný riaditeľ Bezpečnostný technik</p>

ZDROJ: (autor)

11. Prevádzanie jednotlivých skúšok je definované podľa minimálneho rozsahu pre vedúcich zamestnancov jedenkrát za tri roky, pričom musí dôjsť k preskúšaniam od certifikovaného lektora, a to písomným testom. Výsledok je uvedený v Zázname o školení, ktorý je uložený do zložky daného zamestnanca.
12. Ostatní zamestnanci musia byť preskúšaní minimálne jedenkrát za dva roky, a to za prítomnosti certifikovaného lektora a to ústnou formou skúšky. Zamestnanec musí zodpovedať na dve vybrané otázky, ktoré si vyberie náhodne. Výsledok je uvedený v dokumente Záznam o školení, ktorý je uložený do zložky zamestnanca.
13. Uvedená periodicita je minimálna a k jej upravovaniu dochádza v ročných plánoch školení, ktoré sú stanovené na základe predchádzajúcej bilancie percentuálneho rizika vzniku úrazu a hrozby minulého roku.

5.6.1 Osobné ochranné a hygienické pomôcky v organizáciách

Osobné ochranné a hygienické pomôcky musia byť definované vnútorným predpisom. V prípade, že nie je možné riziká odstrániť, alebo dostatočne obmedziť za pomoci aplikovateľnosti opatrení na organizáciu pracovných pozícií, je firma povinná poskytnúť zamestnancovi osobné ochranné pracovné prostriedky.

Tab. 39. Definovanie potreby osobných ochranných a hygienických pomôcok

Definovaná ochranná pomôcka	Pracovná pozícia	Odôvodnenie
Helma	Technik	<ul style="list-style-type: none"> • Pohyb po objekte v čase montáže • Montáž • Revízia • Odstránenie poruchy
Pracovné oblečenie (nohavice, rukavice, vhodná obuv, bunda) Definované v karte pracovnej pozície	Technik	<ul style="list-style-type: none"> • Montáž • Odstránenie závady
Bezpečnostné okuliare	Technik	<ul style="list-style-type: none"> • Montáž • V prípade nebezpečenstva poranenia oka
Istenie (Zdvíhacia plošina pre práce vo výške)	Technik	<ul style="list-style-type: none"> • Montáž • Definuje vedúci pracovník (Technický riaditeľ) v popise pracovnej pozície, v sekcii výkon jednotlivých úloh
Hygienické prostriedky a materiál	Pracovníci upratovacieho režimu	<ul style="list-style-type: none"> • Upratovanie priestorov • Definuje vedúci pracovník (Manažér monitorovacieho centra) v popise pracovnej pozície, popis výkonu práce pre jednotlivých klientov • Pravidelné porady prezentovania pracovného postupu
A iné ...	Definované pri zostavovaní popisu jednotlivých pracovných pozícií	

ZDROJ: (autor)

5.6.2 Požiarna ochrana v organizácií

Podľa zákona č. 133/ 1985 Sb. o požiarnej ochrane, v spoločnosti zodpovedá za organizáciu a zaistenie požiarnej ochrany štatutárny zástupca spoločnosti, a to v rozsahu, ktorý je stanovený zákonom o požiarnej ochrane.

Návrh smernice pre požiarnu ochranu:

1. Zamestnanci vo vedúcich pracovných pozíciách v spoločnosti zodpovedajú za zabezpečenie úloh a povinností na úseku požiarnej ochrany podľa vykonávanej pracovnej funkcie, a to v rozsahu stanovenom vnútorným predpisom o požiarnej ochrane.
2. Organizácia musí mať definovaný samostatný dokument (Tematický plán), ktorý definuje školenia zamestnancov a vedúcich zamestnancov v oblasti požiarnej ochrany, a to podľa aktuálneho rozvrhu školení a za prítomnosti odborne spôsobilej osoby.
3. Každý externý pracovník musí byť oboznámený s konkrétnymi požiadavkami jednotlivých pracovísk na požiarnu ochranu.
4. Každý objekt patriaci spoločnosti musí byť vybavený prostriedkami požiarnej ochrany a požiarne bezpečnostnými zariadeniami podľa projektu. Uvedené prostriedky musia byť pravidelne kontrolované a udržiavané v prevádzkovom stave.
5. Každý objekt musí mať zreteľne označené telefónne číslo tiesňového volania a súčasne aj pokyny pre ohlásenie požiaru. (Verejne dostupné požiarne poplachové smernice)
6. Požiarna dokumentácia musí byť spracovaná odborne spôsobilou osobou, ktorá bude pravidelne uvedenú dokumentáciu aktualizovať a aplikovať do uvedenej dokumentácie prípadné zmeny v požiarnej ochrane určené zákonom, alebo potrebou zmeny z dôvodu zmeny podmienok pracovného prostredia.
7. Zodpovedný pracovník musí pravidelne kontrolovať dodržiavanie daných podmienok a v prípade vyskytnutia poruchy je nevyhnutné, aby došlo ku definovaniu termínu a osoby, ktorá má danú poruchu odstrániť, pričom zodpovedná osoba musí dohliadať nad naplnenie uvedenej podmienky.

8. Stanovením zodpovedností musí dôjsť k definovaniu kompetencií pre osoby zodpovedné za plnenie zákonných podmienok o požiarnej ochrane.
9. Orgán štátneho požiarneho dozoru v určitých intervaloch prevádza kontroly nad dodržiavaním zákonných podmienok na požiarnu ochranu.
10. Vedúci pracovník je povinný zúčastňovať sa pravidelných školení v oblasti požiarnej ochrany a súčasne sa podrobovať testom znalostí v danom obore.
11. Vedúci pracovník je povinný organizovať opakované školenia zamestnancov v oblasti požiarnej ochrany, a to vždy v stanovených intervaloch, ktoré stanovila osoba zodpovedná za požiarnu ochranu.
12. Vedúci pracovníci sú povinný kontrolovať dodržiavanie predpisov požiarnej ochrany a zaistiť viditeľné sprístupnenie dokumentácie požiarnej ochrany.
13. Vedúci pracovník je ďalej povinný zaistiť kontroly na zverenom úseku, vrátane revízií a v prípade vzniku poruchy je povinný umožniť odstránenie poruchy a to v čo najkratšom časovom intervale.
14. Vedúci pracovník je zodpovedný za oznámenie každej skutočnosti, ktorá mohla spôsobiť vyvolanie požiaru, alebo daný požiar vyvolala. Je ďalej zodpovedný za likvidačné práce, v prípade vzniku požiaru za evakuačné plnenie plánu a zaistenie iných prác pre odstránenie požiaru.
15. Každý zamestnanec je povinný zúčastňovať sa uvedených školení a aplikovať školiace procesy v oblasti požiarnej ochrany do každodenného pracovného procesu.
16. V prípade, že zamestnanec odhalí nedostatok na pracovisku, je povinný bezodkladne danú skutočnosť nahlásiť priamemu nadriadenému.
17. Zamestnanec je povinný udržiavať trvalo voľné únikové cesty a cesty k hasiacim zariadeniam.
18. Hlavnou zodpovednou osobou je preventista požiarnej ochrany, ktorý je zodpovedný za značenie pracoviska, kontrolovanie, školenie a vedenie požiarnej knihy.
19. V oblasti požiarnej ochrany musí byť evidovaná dokumentácia požiarnej ochrany, ktorá je definovaná vyhláškou č. 246/ 2001 Sb.

5.7 Definovanie dokumentácie pre plánovanie

Uvedený druh dokumentácie špecifikuje požiadavky normy, ktorej certifikáciu v budúcom vývoji firmy predpokladá vedenie spoločnosti. Jedná sa o certifikáciu podľa ISO 9001. Uvedená časť by mala definovať základné dokumenty, ktoré bude potrebné definovať pred samotným auditom, ktorý bude rozhodovať o udelení certifikácie.

5.7.1 Všeobecné požiadavky na systém manažérstva kvality

Všeobecné požiadavky na systém manažérstva kvality definujú požiadavky normy, ktoré identifikujú miesta, kde v súčasnej dobe spoločnosť nedefinuje uvedené opatrenia na zlepšenie. Uvedená tabuľka je definovaná, ako kontrolný zoznam, ktorý identifikuje, či dochádza k naplneniu určitej požiadavky.

Tab. 40. Hodnotiaci zoznam na požiadavky normy ISO 9001 Všeobecné požiadavky

<i>Požiadavka NORMY na udržanie systému manažérstva kvality</i>	<i>Hodnotenie Splňuje / Nesplňuje</i>	
• Musí dôjsť k identifikácii používania procesov manažérstva kvality		
• Musí dôjsť ku stanoveniu postupnosti jednotlivých procesov a ich vzájomný účinok		
- Stanovenie metód pre realizáciu a riadenie jednotlivých procesov		
- Dostupné zdroje a informácie pre podporu a hodnotenie procesov		
• Musí dochádzať k pravidelnej kontrole a analýze procesov		
- Prijat' opatrenia, ktoré budú zabezpečovať neustále zlepšovanie		
• Zabezpečiť operatívne riadenie vyčlenených procesov		

ZDROJ: (autor)

Nasledujúca tabuľka je definovaná, ako kontrolný zoznam, ktorý identifikuje chýbajúcu dokumentáciu v procese hodnotenia požiadaviek pre ISO 9001. Hodnotenie stanovuje dva hodnotiace výrazy, a to či organizácia disponuje danou dokumentáciou, alebo nedisponuje. Ak uvedená organizácia nedisponuje uvedenou dokumentáciou je potrebné určiť termín, kedy bude prejednávané spracovanie dokumentácie, pričom dôjde aj k určeniu kompetentných osôb.

Tab. 41. Hodnotiaci zoznam na dokumentáciu ISO 9001 Všeobecné požiadavky

<i>Dokumentácia</i>	<i>Hodnotenie</i>		
	<i>Disponuje</i>	<i>Nedisponuje</i>	<i>Termín</i>
Príručka manažérstva kvality			
Smernice o pracovných postupoch			
Vývojové diagramy procesov			
Investičné plány			
Plány činnosti			
Manažment posúdenia			

ZDROJ: (autor)

5.7.2 Požadavky na dokumentáciu systému manažérstva kvality

Všeobecné požiadavky normy definujú, že organizácia musí mať definovanú politiku a ciele kvality, príručku kvality, podklady potrebné na riadenie procesu, postupy zdokumentované podľa tejto normy a záznamy o kvalite. Uvedený kontrolný zoznam definuje nevýrobnú dokumentáciu, ktorá v prípade výroby musí byť doplnená o ďalšie postupy. Jedná sa o upravenie dokumentácia o výrobnom procese do procesu firmy a cieľu podnikania, vzhľadom na skutočnosť, že spoločnosť má strategický cieľ do budúceho vývoja, ktorý definuje vlastnú výrobu uvedených komponentov. V súčasnosti ale dochádza k absencií dokumentu, ktorý by charakterizoval súčasný stav podniku a definoval by presné pravidlá riadenia jednotlivých procesov, a to za účelom riadenia rizík a procesu neustáleho zlepšovania.

Návrh hodnotenia je rovnaký, ako v predošlej podkapitole, kde dochádzalo k určeniu, či organizácia v súčasnosti daný dokument má, a ak nie kedy bude prejednávané jeho plánovanie, nejedná sa o termín, kedy má daný dokument byť zostavený, ale kedy bude jednanie o danom dokumente.

Tab. 42. Hodnotiaci kontrolný zoznam na potrebnú dokumentáciu

Dokumentácia	Hodnotenie		
	Disponuje	Nedisponuje	Termín
Príručka manažérstva kvality			
Smernice o procesoch a postupoch			
Závazok stáleho zlepšovania			
Neustále hodnotenie			
Postup informácií v rámci organizácie			
Popis vzájomných účinkov			
Skúšobné plány			
Vývojové diagramy procesu			
Výkresy			
Organigramy			
Smernica o riadení dokumentácie			
Smernica o záznamov o kvalite			
Smernica o riadení interných auditov			
Smernica o riadení nezhodného produktu – Reklamácia dodávky			
Smernica o riadení nápravných činností			
Smernica o riadení preventívnych činností			
Záznamy objednávok			
Výrobné výkazy – Nevýrobný proces – Inštalačné výkazy			
Protokoly – O skúškach inštalácie, reklamácie			
Katalógové listy			
Doklady o skúškach – Nevýrobný proces			
Doklady o spôsobilosti			

ZDROJ: (autor)

Tab. 44. Návrh kontrolného zoznamu pre Závazok manažmentu

Dokumentácia Závazku manažmentu	Hodnotenie		
	Disponuje	Nedisponuje	Termín
Zápisy o politike kvality			
Plány školení / doklady o školeniach			
Informovanie pracovníkov (vyhlášky, programy informatívnych podujatí)			
Plány rozvoja personálu			
Plány manažérstva kvality			
Zápisy o stanovených hodnotách			
Projekty			
Investičné plány			
Podnikové dohody			

ZDROJ: (autor)

Zameranie na zákazníka je určitý aspekt, ktorý pre získanie kvality musí byť dodržaný, teda v hlavnej roli musí byť zákazník a zisťovanie jeho potrieb a požiadaviek. Dochádza ku definovaniu dokumentov, ktoré definujú očakávania, potreby a požiadavky klientov.

Tab. 45. Návrh kontrolného záznamu pre Zameranie na zákazníka

Dokumentácia Zamerania na zákazníka	Hodnotenie		
	Disponuje	Nedisponuje	Termín
Vyhodnotenie otázok zákazníka			
Analýza trhu			
Dokumentácia o reklamáciách a ich analýza			
Záznamy o validácii produktov			
Externé náklady na kvalitu			
Analýza spokojnosti klientov			

ZDROJ: (autor)

Politika kvality by podľa normy mala definovať, či je vhodná pre danú organizáciu, a to za pomoci definovania záväzku stáleho zlepšovania a vypracovania cieľov kvality, ktoré ale musia byť v organizácii pochopené, inak ich účinnosť bude nulová. Či je daná politika vhodná musí byť v čase preskúmané, ale nemalo by dochádzať k úplnej zmene, len ku zmene na úrovni čiastočnej, pričom dochádza k zmene podľa externých požiadaviek, ktoré sa s časom vyvíjajú.

Plánovanie by malo byť navrhované do budúceho vývoja, a to tak, aby nedochádzalo ku porušeniu integrity systému manažérstva kvality uvedenej organizácie. Plány by mali byť definované v každej oblasti, v ktorej podnik vykonáva činnosť. V prípade zavedenia výroby sa samozrejme plány rozsiahlo zvýšia, ale v prípade, že spoločnosť nevyrába ale chce splňovať dané podmienky, tak musí aj externý dodávateľ splňovať podmienky certifikácie, ktoré organizácia zabezpečí pomocou určenia zmluvných vzťahov.

Jedným z ďalších požiadaviek je stanovenie procesu definovania zodpovedností a právomocí, pričom úzko s danou témou súvisí definovanie pracovných miest a funkcií spolu s definovaním profilu jednotlivých požadovaných skúseností na danej pozícii. Ak daná

osoba nemá uvedené znalosti a skúsenosti, ale uvedenú funkciu už nejakú dobu vykonáva, dochádza ku procesu naplánovania vzdelania tak, aby uvedené požiadavky splňovala v určitom časovom intervale. Predstavitel' manažmentu reprezentuje nezávislého člena manažmentu, ktorý zavádza celý systém manažérstva kvality do procesu firmy a spracováva správy vrcholnému manažmentu, čím dochádza k naplneniu požiadavky informovanosti o požiadavkách zákazníka.

Tab. 46. Návrh kontrolného zoznamu dokumentu pre Internú komunikáciu

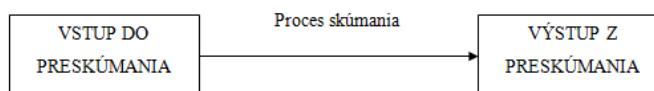
Dokumentácia Interná komunikácia	Hodnotenie		
	Disponuje	Nedisponuje	Termín
Protokoly a správy z rokovaní			
Skupinové školenia			
Návesné tabule, časopisy			
Audiovizuálne a elektronické médiá			
Programy podnikových podujatí			
Štatistiky			
Správy o efektívnosti systému manažérstva kvality			

ZDROJ: (autor)

Interná komunikácia je charakteristická pre nastavenie komunikácie vo internom prostredí podniku. Hlavnou úlohou normy je definovať požiadavky na vytvorenie príslušných komunikačných kanálov v rámci organizácie, pričom musí byť kladený dôraz na efektívnosť komunikácie v systéme manažérstva kvality. Zjednodušene to znamená, že pokiaľ firma chce zlepšiť kvalitu poskytovaných služieb, musí každý článok podniku rozumieť uvedenej stratégii.

5.7.4 Požiadavky na systém preskúmania manažmentom

Preskúmanie manažmentom je v organizáciách zavádzané pre zavedenie procesu, ktorý pravidelne preskúmava systém manažérstva kvality, a to z dôvodu, aby bol efektívny a funkčný. Uvedeným preskúmaním dochádza ku zhodnoteniu príležitostí na zlepšenie, a teda k jednoduchšej implementácii do procesu.



Obr. 53. Proces preskúmania manažmentom

ZDROJ: (autor)

Uvedené preskúmanie je opakované po určitom časovom intervale, ktorý je určený v procese plánovania, teda dochádza ku stanoveniu intervalu. Jedná sa o preskúmanie vstupov, ktoré na konci skúmania budú definovať výstupy, ktoré sa budú podieľať na procese zlepšovania.

5.7.5 Požiadavky na ľudské zdroje

Každý pracovník, ktorý vykonáva v podniku určitú funkciu, sa podieľa na procese ovplyvňujúcom kvalitu produktu, alebo poskytovanej služby. Dochádzame k záveru potreby definovať vzdelanie, prípravu, zručnosti a skúsenosti na uvedené pracovné pozície. V procese kompetentnosti musí dochádzať k definovaniu potreby určitej prípravy, ale hlavne k definovaniu spôsobu, akým bude dochádzať k jej naplneniu. Následne musí dochádzať k preskúmaniu efektívnosti danej prípravy a udržiavaniu primeraných záznamov o danom procese.

Tab. 47. Návrh kontrolného zoznamu na dokumentáciu prípravy zamestnancov

<i>Dokumentácia prípravy zamestnancov</i>	<i>Hodnotenie</i>		
	<i>Disponuje</i>	<i>Nedisponuje</i>	<i>Termín</i>
Popisy pracovných miest			
Pracovné zmluvy			
Plány vývoja zamestnancov			
Osvedčenia o kvalifikácii			
Záznamy s rozhovorov zo zamestnancami			
Vysvedčenia pracovníkov			
Kvalifikačné matice			
Doklady o príprave zamestnancov			
Analýza spokojnosti pracovníkov			
Analýza neprítomnosti			
Doklady o poučení o ochrane pri práci			

ZDROJ: (autor)

5.7.6 Požiadavky na systém realizácie produktu

Uvedené požiadavky sú aplikované na produkt, v našom prípade na poskytovanie služby. Aj keď nedochádza k výrobe, dochádza k poskytnutiu služieb, ktoré vytvárajú produkt uvedenej organizácie, alebo podniku. V konečnom dôsledku dochádza ku vytvoreniu produktu.

Tab. 48. Návrh kontrolného zoznamu pre Realizáciu produktu

<i>Dokumentácia na realizáciu produktu</i>	<i>Hodnotenie</i>		
	<i>Disponuje</i>	<i>Nedisponuje</i>	<i>Termin</i>
Plánovanie realizácie produktu / služby			
Procesy dotýkajúce sa zákazníka			
Určenie požiadaviek na produkt / službu			
Preskúmanie požiadaviek na produkt / službu			
Komunikácia so zákazníkom			
Spätná väzba			

ZDROJ: (autor)

5.7.7 Požiadavky na návrh a vývoj

Pri definovaní požiadaviek na návrh a vývoj produktu, alebo služby je nutné určiť aspekty spojené s jednotlivými etapami návrhu a vývoja, musí dochádzať k definovaniu pravidiel verifikácie a validácie, definovať právomoci a zodpovednosti a pravidelne aktualizovať plány. Pre vstup do procesu je potrebné definovať požiadavky na funkciu a výkonnosť a súčasne definovať požiadavky predpisov a legislatívnych dokumentov. Pri hodnotení daného návrhu by mali byť zohľadňované iné podobné návrhy, alebo by sa malo prihliadať k predchádzajúcim návrhom daného vývojového plánu. Pre vstup je tiež dôležité stanoviť proces reklamácie a recyklácie.

Tab. 49. Návrh kontrolného zoznamu pre návrh a vývoj produktu/ služby

<i>Dokumentácia pre návrh a vývoj</i>	<i>Hodnotenie</i>		
	<i>Disponuje</i>	<i>Nedisponuje</i>	<i>Termin</i>
Plánovanie návrhu vývoja			
Vstup do návrhu a vývoja			
Výstupy z návrhu a vývoja			
Preskúmanie návrhu a vývoja			
Verifikácia návrhu a vývoja			
Validácia			
Riadenie zmien návrhu a vývoja			

ZDROJ: (autor)

Každý výstup by mal spĺňať podmienky na vstupe, ale aj by malo dochádzať k popisu vyhodnotenia schopnosti plniť požiadavky, ktoré na daný produkt boli v čase návrhu kladené. Súčasťou dokumentácie sú laboratórne skúšky, v prípade služby sa jedná o simuláciu živého prostredia, simulácie predvídaných skutočností a iné pre daný návrh dôležité pôsobiace aspekty. Validácia by mala v súlade s plánovanými pravidlami potvrdzovať, že je zabezpečená spôsobilosť použitia a potrebná dokumentácia k produktu.

5.7.8 Požiadavky na systém nákupu

V procese nakupovania musí dochádzať ku hodnoteniu a výberu dodávateľa určitého produktu. Na proces hodnotenia musí dôjsť k stanoveniu kritérií. V procese rozhodovania dochádza k zohľadňovaniu nasledujúcich požiadaviek:

- Vonkajšia kvalita produktu,
- Vplyvy na podnik,
- Spôsobilosť dodávateľa,
- Dokumentácia hodnotenia.

Tab. 50. Návrh kontrolného zoznamu pre proces výberu dodávateľa

Dokumentácia procesu výberu Dodávateľa	Hodnotenie		
	Disponuje	Nedisponuje	Termín
Špecifikácie produktov			
Dokumentácia kvality dodávateľa			
Katalógový list			
Doklady o hodnotení dodávateľa			
Databáza schválených dodávateľov			
Kritériá hodnotenia dodávateľov			
Procesy reklamácie			
Dohody o kvalite			
Požiadavkové listy			
Objednávkové listy			
Dohody na zabezpečenie kvality			
Písomné doklady o schválení objednávky			

ZDROJ: (autor)

Pre verifikáciu nákupného produktu je nutné vypracovať dokumentáciu pre zavedenie kontroly, ktorá overuje splnenie požiadaviek, ktoré boli určené dodávateľovi, pri zadaní požiadavky na produkt. Pri procese verifikácie dodávateľa je nutné určiť stanovené metódy verifikácie a skúšobné predpisy, ktoré sú využívané pre vstupnú kontrolu nakupovaného tovaru.

5.7.9 Požiadavky na výrobu a poskytovanie služieb

Je potrebné stanoviť charakteristiku produktu, pričom je nutné zabezpečiť dostupnosť pracovných inštrukcií, definovať vhodné zariadenia, definovať monitorovacie nástroje a zabezpečiť dodávku služby. Validácia procesov by mala potvrdiť spôsobilosť postupov, pričom by malo dochádzať k zohľadňovaniu pracovných postupov, ktorých výsledky nie je možné overiť validáciou, ale ich nedostatky sa prejavajú až v prípade dodania služby zákazníkovi.

V procese, kedy hovoríme o uvedenej firme, pre ktorú sa dotýkajú pravidlá stanovované uvedeným dokumentom, je nutné brať do úvahy majetok zákazníka, pretože vo väčšine

případov pri dodávke služby, alebo produktu dochádza ku kontaktu pracovníka organizácie s daným majetkom.

Tab. 51. Návrh kontrolného zoznamu pre výrobu a poskytovanie služieb

Dokumentácia procesu výroby a poskytovania služieb	Hodnotenie		
	Disponuje	Nedisponuje	Termín
Riadenie výroby a poskytovania služieb			
Kritéria prijatia			
Výkresy			
Plány			
Vývojové diagramy procesu			
Validácia procesov výroby a poskytovania služieb			
Popisy procesov			
Dokumentácia školení			
Doklady o kvalifikácii			
Identifikácia a sledovateľnosť			
Pracovné pokyny			
Sprievodné listy			
Majetok zákazníka			
Ochrana produktu (kvality služby)			

ZDROJ: (autor)

Jedná sa o stanovenie takých opatrení, ktoré pre budúci vývoj v procese zavedenia výroby stanovujú základné princípy. Teda v súčasnosti sa jedná o produkt služby, ktorý je poskytovaný danou organizáciou, pre budúci vývoj je do procesu počítané s implementáciou ďalších produktových požiadaviek.

5.8 Definovanie smerníc pre meranie, analýzy a zlepšovanie

Pre definovanie procesov merania, analýz a zlepšovania je všeobecne platná podmienka, že by malo dochádzať k neustálemu zlepšovaniu a to stanovením daných smerníc, ich plánovaniu, teda plánovaniu jednotlivých krokov a ich zavádzaniu do praxe podniku.

Tab. 52. Návrh kontrolného zoznamu pre meranie, analýzy a zlepšovanie

Dokumentácia procesu Merania, analýzy, zlepšovania	Hodnotenie		
	Disponuje	Nedisponuje	Termín
Monitorovanie a meranie			
Spokojnosť zákazníka			
Interný audit			
Monitorovanie a meranie procesov, produktu, služby			
Riadenie nezhodného produktu			
Analýza údajov			
Zlepšovanie			
Trvalé zlepšovanie			
Nápravná činnosť			
Preventívna činnosť			

ZDROJ: (autor)

V prípade produktu je nutné proces produktu, alebo poskytnutia služby monitorovať, merať, overovať a zaznamenávať, a to v primeraných časových etapách realizácie, pričom

vždy musí dochádzať k uvedeniu zodpovednej osoby za daný segment. V prípade mimoriadneho uvoľnenia produktu zo strany zákazníka je potrebné o tom spracovať zápis.

V prípade nezhodného produktu by mali byť uvedené produkty identifikované, oddelené od zhodných produktov, riadené, musí dôjsť ku odstráneniu nezhody, znovu overenie a zaznamenanie. Opravené produkty musia byť znovu overované, alebo mimoriadne uvoľnené zo strany zákazníka, o čom musí byť spísaný dokumentačný záznam.

6 APLIKÁCIA A HODNOTENIE NAVRHOVANÝCH POSTUPOV A CIELOV BEZPEČNOSTNEJ POLITIKY

Aplikovanie uvedených návrhov do procesu chodu podniku je realizované podľa časového harmonogramu. Návrh časového plánovania pre fyzickú ochranu je zobrazený v prílohovej časti práce, a to pod názvom PRÍLOHA P VIII. Definovanie vzájomného vzťahu väzby procesov je uvedené v prílohovej časti práce pod označením PRÍLOHA P VII. Pod názvom prílohy PRÍLOHA P IX je zobrazené porovnanie vybraných procesov s aplikáciou bezpečnostného pravidla a bez aplikácie uvedeného pravidla, teda proces prebiehajúci pred zavedením daných pravidiel a proces po ich implementovaní.

Hodnotenie navrhovaných postupov a cieľov bezpečnostnej politiky je možné realizovať na troch úrovniach hodnotenia. Hodnotenie primárne ku ktorému dochádza v samotnej fáze návrhu postupov bezpečnostnej politiky a podľa ohodnotenia adekvátneho riešenia dochádza ku stanoveniu bezpečnostných plánov. Sekundárne hodnotenie je rozdelené do niekoľkých fáz, ktoré sú dlhodobu plánované. Je možné ho definovať, ako krátkodobé hodnotenie a hodnotenie dlhodobé. V uvedených hodnoteniach je možné konštatovať, či daná bezpečnostná stratégia splňa svoj cieľ, a ak áno k akému percentuálnemu vyjadreniu z hľadiska plnenia cieľa dochádza.

6.1 Definovanie procesu hodnotenia aplikovaných postupov

Proces hodnotenia je realizovaný dlhodobu a hodnotiace parametre sú pevne stanovené. Ak chceme identifikovať zmenu na úrovni riadenia, je nutné, aby sme aplikovali určité opatrenia do procesu určitý časový interval. Proces hodnotenia je vytváraný parametrami, ktoré sú stále, ale aj mennými parametrami a parametrami inými, ktoré sa vyskytli v procese neplánovane.

Definovanie hodnotenia musí zahrňovať:

- Čo má byť hodnotené – definovanie cieľa,
- Ako bude realizované hodnotenie – výber vhodnej metódy,
- Časový plán kontroly,
- Definovanie vyhodnotenia,

- Definovanie prítomnosti odchýlky, alebo chyby – definovať povolené odchýlky,
- Zodpovednosti za dané hodnotenie,
- Definovanie nápravných opatrení,
- Následné stanovenie časového plánu a opakovanie kontroly.

Navrhovaná bezpečnostná politika má za cieľ uľahčiť vývoj spoločnosti a minimalizovať vznik hrozby, ktorá by priamo, alebo nepriamo ohrozila spoločnosť.

Tab. 53. Návrh pre hodnotenie účinnosti jednotlivých bezpečnostných stratégií

Hodnotený cieľ:					
Dátum implementácie opatrení:		Predpokladaný dátum prvej kontroly:		Skutočný dátum kontroly:	
Definované kontrolné parametre (otázky)	Hodnotenie otázok		Percentuálne vyjadrenie	Povolený interval	Prítomnosť odchýlky

ZDROJ: (autor)

Predpokladaný vývoj aplikovateľnosti je dlhodobý, a podlieha určeniu konkrétnych termínov pre realizáciu. Nasledujúca tabuľka definuje časové intervaly, v ktorých by malo dôjsť k implementovaniu opatrení do chodu podniku.

Tab. 54. Návrh časového plánu pre aplikáciu jednotlivých smerníc do procesu

Fyzická bezpečnosť objektu	Mechanické zábranné prvky	30 dní	80 – 90 dní
	Poplachové zabezpečovacie a tiesňové prvky	30 dní	
	Kamerový systém	21 dní	
Prístupnosť do objektu	Prístupový systém	21 dní	35 – 40 dní
	Definovanie pravidiel prístupu	14 dní	
Personálna bezpečnosť	Aplikácia zamestnaneckých postupov pre výkon práce	7 dní	35 – 40 dní
	Karty zamestnaneckých pozícií	7 dní	
	Plány povinných školení a rekvalifikácií	14 dní	
	Definovanie schvaľovacieho procesu a priamych nadriadených	7 dní	
Informačná bezpečnosť	Zavedenie informačného systému	40 dní	50 – 65 dní
	Definovanie práv pre prácu s dokumentmi	14 dní	

ZDROJ: (autor)

Po uplynutí definovaného intervalu dochádza ku kontrole, ktorá je realizovaná podľa zavedenej smernice. Uvedené smernice sú definované ako vstupný dokument pre stanovenie kontrolných otázok. Plnenie uvedených kontrolných otázok je vyhodnotené podľa definovaného hodnotenia, ktoré stanovuje 100% plnenie ako ideálny stav, podľa závažnosti hodnoteného cieľa je vypočítaná prípustná miera chybovosti. V prípade neprípustnej miery dochádza k určeniu termínu a zvolaniu porady vedenia, kde dôjde k návrhu riešenia na vzniknutý problém.

Tab. 55. Návrh pre vyhodnotenie

	Kontrola v intervale (85 dní)			Kontrola po intervale (100 dní)		
	Hodnotenie	Prípustná miera	STAV	Hodnotenie	Prípustná miera	STAV
Fyzická bezpečnosť objektu	68%	75%	NEG	95%	98%	NEG
Pristupnosť do objektu	74%	75%	NEG	98%	98%	NEG

ZDROJ: (autor)

Stav je definovaný na niekoľkých úrovniach podľa stavu plnenia. Definovanie stavov prebieha podľa percentuálneho určenia predpokladu plnenia a definovanej možnej odchýlky od ideálneho stavu.

Tab. 56. Návrh pre definovanie hodnotenia stavu a vyvodenie záveru

Percentuálne vyjadrenie plnenia požiadaviek	Význam	STAV	Záver
100% -90%	Ideálne plnenie požiadaviek	OK	Stanoviť ďalší proces kontroly do budúceho vývoja
89% - 80%	Plnenie požiadaviek v odchýlke	POZ	Dbať na zlepšenie
79% - 70%	Čiastočné plnenie požiadaviek	Hodnotenie podľa definovanej odchýlky	Definovať nápravné opatrenia
69% - 60%	Plnenie požiadaviek mimo požadovanú úroveň	NEG	Zvolanie porady vedenia - návrh zmeny
59% - 50%	Neplnenie požiadaviek	KO	Vyvodenie záveru – nutná zmena
49% - 40%	Negovanie strategických cieľov spoločnosti	SANKCIA	Definovanie vymáhania sankcií a trestov od kompetentných
39% - 0%	Zlyhanie vedenia	SANKCIA	Definovanie vymáhania sankcií a trestov od kompetentných

ZDROJ: (autor)

Uvedené tabuľky sú do poručujúce a pri stanovovaní kontrolných dokumentov môže byť v patričnej miere hodnotenie pozmenené podľa potreby kontroly. Každá kontrola účinnosti musí byť dokumentovaná a závery musia byť odôvodnené v dostatočnej miere. Pri definovaní hodnotenia je nutné stanoviť vždy odchýlky, s ktorými daná organizácia bude počítať v prípade ďalšieho plánovania. Je dôležité si uvedomiť, že proces dosiahnutia cieľu nie je v zmene cieľa, ale v schopnosti nájsť plán, ktorý dokáže splniť definovaný cieľ.

ZÁVER

Cieľom diplomovej práce bolo analyzovať súčasný stav vybraného podniku, a to za cieľom nájsť potenciálne hrozby, ktoré vybranej organizácii hrozia a následne definovať riadenie uvedených rizík.

Teoretická časť práce popisuje jednotlivé metódy pre analyzovanie bezpečnostných rizík a súčasne popisuje definované praktiky pre zostavenie bezpečnostnej organizácie. Teoretické poznatky z uvedenej časti práce sú následne aplikované do praktického hodnotenia vybranej organizácie.

Praktická časť práce je primárne rozdelená na tri časti, ktoré sú tvorené popisom vybraného subjektu, analytickým procesom a zhodnotením a následným návrhom riešenia. Popis organizácie obsahuje prvky štruktúry, ktorá bola navrhovaná pre danú bezpečnostnú politiku, vzhľadom na získané informácie. Pri hodnotení uvedenej organizácie dochádzalo ku všeobecnému pohľadu na organizáciu, pričom dochádzalo k zohľadňovaniu strategických plánov spoločnosti do budúceho vývoja. V analytickej časti dochádzalo k implementácii poznatkov a analytických metód z teoretickej časti, a to za cieľom získania výsledného hodnotenia. Uvedené metódy boli navrhované pre ďalšie kontrolné hodnotenie v priebehu aplikovania jednotlivých riešení do chodu organizácie. Hodnotenie prebiehalo definovaním metódy na hodnotenie a následne definovaným parametru, podľa ktorého sa hodnotenie odvíjalo. Pri definovaní záverov a formulácií rizík dochádzalo k využívaniu metódy prognózovania negatívneho stavu a následné stanovenie pre riadenie daného rizika. V návrhovej časti práce dochádzalo k navrhnutiu riadenia rizík, a to definovaním bezpečnostnej politiky organizácie. Bezpečnostná politika definovala smernice, ktoré by v internom prostredí organizácie mali byť dodržiavané. V závere práce dochádzalo k popisu aplikovateľnosti návrhových riešení do príkladových situácií, ktoré mali za úlohu zobrazit' rozdielne pôsobenie na bezpečnosť organizácie. V časti práce hodnotenia dochádzalo k návrhu časových intervalov, ktoré by mali byť stanovené na jednotlivé bezpečnostné plány, aby bolo možné kontrolovať dosiahnuteľnosť vytýčeného cieľa, a súčasne dochádzalo k definovaniu stavov, ktoré vyplývajú z percentuálneho vyjadrenia plnenia definovaných plánov.

V prípade vybranej organizácie sa jedná o dlhodobé zmeny, ktoré musia byť trvalo uznávané vedením spoločnosti, aby aplikovanie uvedených stratégií malo význam pre budúci

vývoj firmy. Je nutné poznamenat, že navrhovanú bezpečnostnú politiku je nutné implementovať do organizácie s časovým plánom a určením zodpovednosti kompetentných osôb. Je nevyhnutné, aby uvedené stratégie boli pochopené celou firmou, a teda aby bola zaručená ich správna implementácia do jednotlivých prípadov, pretože vytvoriť silný systém musíme od základného kameňa spoločnosti, a teda od zamestnancov.

ZÁVER V ANGLIČTINE

The aim of the thesis was to analyze the current status of the selected company, in order to identify potential threats to selected threatened organization and then define the management of those risks.

The theoretical part describes various methods for analyzing security risks and describes the current defined practices for establishing security organization. Theoretical knowledge of that part of the work is then applied to the practical evaluation of selected organizations.

The practical part is primarily divided into three parts, which consist of a description of the selected operator, and analysis and assessment, and then propose solutions. Description of the organization includes structural elements, which has been proposed for a given security policy, based on the information obtained. In the evaluation of the organization took place in a general view of the organization, while there was a taking into account of the strategic plans for the future development. In the analytical part occurred on the implementation of knowledge and analysis of a theoretical part, for the purpose of obtaining a final assessment. Those methods have been proposed for the evaluation of other control over the application of different solutions to the running of the organization. Assessment was carried out by defining methods to assess and subsequently defined parameters under which the evaluation unwound. When defining the formulation of conclusions and there was a risk forecasting methods use the negative state and the subsequent determination of risk management. The design part of the work there was to propose risk management by defining security policy of the organization. Security policies define directive, which in the internal environment of the organization should be followed. In conclusion there was a description of the applicability of exemplary design solutions to situations that had the task show different effects on the security of the organization. Under Labour there was a proposal evaluation periods, which should be set for individual security plans, in order to check attain desired goal while there was to define conditions that result from implementation of the rate defined plans .

In the case of the body selected is a long-term change that needs to be permanently by manager, the application of these strategies, in order to be relevant for the future development of the company. It should be noted that the proposed security policy must be implemented in organizations with a timetable and determining liability competent persons. It is essential that those strategies have been understood by employees, and therefore, to

ensure their proper implementation in individual cases, because we create a strong system of foundation stone company, and the employees.

ZOZNAM POUŽITÉJ LITERATURY

- [1] BRABEC, František. Bezpečnost pro firmu, úřad, občana. Praha: Public History, 2001, 400 s. ISBN 80-86445-04-6
- [2] BRABEC, F.: Ochrana bezpečnosti podniku, 1. vydání, Praha: EUROUNION, 1996, 204 str., ISBN 80-85858-29-0.
- [3] BRABEC, František. Hlídací služby. Praha: Eurounion, 1995, 259 s. ISBN 8085858126.
- [4] BUGANOVÁ, K. a kol.: 2012. Manažment rizika v podniku. 1. vyd. Žilina: Žilinská univerzita v Žiline. 2012. ISBN 978-80554-0459-2.
- [5] HÁLEK, Vítězslav. Krizový management: aplikace při řízení podniku. 1. vyd. Hradec Králové: Gaudeamus, 2006, 317 s. ISBN 80-7041-248-8.
- [6] HUDÁKOVÁ, M. a kol.: 2013. Metódy a techniky v procese manažmentu rizika. 1. vyd. Žilina: Žilinská univerzita v Žiline. 2013. ISBN 978-80554-0642-8.
- [7] HURTA, Josef a Vladimír LAUCKÝ. Management bezpečnostního inženýrství. Vyd. 1. Zlín: Univerzita Tomáše Bati, 2006, 172 s. ISBN 80-7318-412-5.
- [8] KAMENÍK, J., BRABEC, F. a kol.: Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur, 1. vydání, Praha: ASPI, a.s., 2007, 340 str., ISBN 978-80-7357-309-6.
- [9] KLUČKA, J.: 2013. Planning and Forecasting. 1st edition. Žilina: Žilinská univerzita v Žiline. 2013. ISBN 978-80554-0653-4
- [10] KONÍČEK, Tomáš, Pavel KOCÁBEK a Stanislav KŘEČEK. Městské kamerové dohlížecí systémy. Praha: Odbor prevence kriminality Ministerstva vnitra ČR, 2002, 87 s., s. obr. příl. ISBN 8073120097.
- [11] KUBÍČKOVÁ, Lea a Karel RAIS. Řízení změn ve firmách a jiných organizacích. 1. vyd. Praha: Grada, 2012, 133 s. ISBN 978-80-247-4564-0
- [12] LÁTAL, I., ŠTAJNERSKÝ, M.: Bezpečnostní zásady ochrany podniku: prevence a řešení krizových situací, 4. vydání, Praha: PROSPEKTUM, 2001, 120 str., ISBN 80-7175-091-3.
- [13] LAUCKÝ, V.: Technologie komerční bezpečnosti II, 1. vydání, Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 123 str., ISBN 80-7318-231-9.
- [14] LUKÁŠ, Luděk a KOLEKTIV. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.
- [15] LUKÁŠ, Luděk, Petr HRŮZA a Milan KNÝ. Informační management v bezpečnostních složkách. 1. vyd. Praha: Ministerstvo obrany České republiky, 2008, 214 s. ISBN 978-80-7278-460-8.
- [16] PROCHÁZKOVÁ, Dana. Bezpečnost lidského systému. 1. vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2007, 139 s. ISBN 978-80-86634-97-5.
- [17] RAIS, Roman. Specifika krizového managementu. Vyd. 1. Ostrava: Key Publishing, 2007, 92 s. ISBN 978-80-87071-11-3.

[18] VAŠINA, Tomáš. Návrh bezpečnostní politiky vybrané bioplynové stanice. Zlín, 2013. diplomová práce (Ing.). Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky

[19] VEJDĚLEK, Jiří. Jak zlepšit podnikové plánování. 1. vyd. Praha: Grada, 1999, 100 s. ISBN 8071696668.

[20] ZÁNICKÁ HOLÁ, K. - Ristvej, J. - Šimák, L.: Posudzovanie rizík priemyselných procesov: Iura Edition, Bratislava, 2010, ISBN: 978-80-8078-344-0.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

BOZP	Bezpečnosť a ochrana zdravia pri práci
CLA	Check List Analysis
RT	Routine Tests
SA	Safety audit
SWOT	Strengths, Weaknesses, Opportunities, Threats
PHA	Preliminary Hazard Analysis
HAZOP	Hazard and Operability Study
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FTA	Fault Tree Analysis
HTA	Hazard Tree analysis
CCA	Cause Consequence Analysis
HRA	Human Reliability Analysis

ZOZNAM OBRÁZKOV

Obr. 1. Rozdelenie systému bezpečnostnej politiky podniku na subsystém [2]	18
Obr. 2. Definovanie druhov ochrany podniku [12].....	18
Obr. 3. Definovanie povahy straty [12]	19
Obr. 4. Vzťah miery zabezpečenia na miere ohrozenia [1]	21
Obr. 5. Rozdelenie typológie prognózovania [2]	24
Obr. 6. Kvantitatívne a kvalitatívne metódy analýzy rizík [6]	26
Obr. 7. Výpočet miery rizika podľa kvantitatívnej metódy [4]	27
Obr. 8. Indukčné a dedukčné metódy analýzy rizík [6]	27
Obr. 9. Primárne metódy používané na analýzu rizík [16].....	28
Obr. 10. Definovanie analýzy SWOT [16].....	29
Obr. 11. Definovanie primárnych smerov analýzy príčin a následkov [16].....	34
Obr. 12. Vzor aplikácie analytického vyhodnotenia pomocou krízovej matice	36
Obr. 13. Vzorové spracovanie maticovej metódy vyhodnotenia rizika	37
Obr. 14. Primárne ciele organizácie.....	42
Obr. 15. Základné rozdelenie spoločnosti.....	43
Obr. 16. Základné zobrazenie funkcií obchodného oddelenia.....	44
Obr. 17. Základné definovanie technického oddelenia	45
Obr. 18. Definovanie analytickej činnosti technického oddelenia.....	45
Obr. 19. Definovanie inštalačných činností technického oddelenia	46
Obr. 20. Definovanie činností servisu technického oddelenia	46
Obr. 21. Definovanie monitorovacích funkcií technického oddelenia	47
Obr. 22. Charakteristika oddelenia bezpečnostného manažmentu	47
Obr. 23. Charakteristika oddelenia informačnej bezpečnosti	48
Obr. 24. Charakteristika ekonomického oddelenia.....	48
Obr. 25. Charakteristika funkcií právneho oddelenia.....	49
Obr. 26. Charakteristika funkcií personálneho oddelenia	49
Obr. 27. Lokalizácia jednotlivých monitorovacích miest a pôsobnosti spoločnosti	50
Obr. 28. Definovanie jednotlivých pobočiek a ich funkcia v lokalizácií.....	51
Obr. 29. Definovanie spôsobu vedenia v organizácií.....	53
Obr. 30. Popis jednotlivých obchodných pozícií Praha.....	54
Obr. 31. Popis jednotlivých obchodných pozícií Brno.....	55

Obr. 32. Popis jednotlivých technických pozícií.....	56
Obr. 33. Popis vedenia vedúcim audítorom	57
Obr. 34. Defínovanie vzťahu výjazdovej hliadky a vedenie	57
Obr. 35. Znázornenie vedenia zo strany manažéra monitorovacieho centra	58
Obr. 36. Defínovanie potrieb zákazníka vzhľadom ku organizácií.....	59
Obr. 37. Defínovanie procesu objednávky služby zákazníka	60
Obr. 38. Diagram reprezentujúci pracovné činnosti na zákazke	61
Obr. 39. Defínovanie primárnych cieľov bezpečnostnej politiky.....	64
Obr. 40. Defínovanie vyhodnoteného vzťahu stupnice zranení a ich počet	69
Obr. 41. Defínovanie vyhodnotenia stupnice hodnotenia početnosti zranení.....	69
Obr. 43. Analýza vplyvom porúch a následkov.....	72
Obr. 44. Proces získania klienta	73
Obr. 45. Proces tvorby projektu po získaní zákazky	73
Obr. 46. Využitie diagramu pre modelovanie.....	84
Obr. 47. Zobrazenie základných strategických cieľov do budúceho vývoja organizácie.....	86
Obr. 48. Diagram hodnotenia nasadenia uvedených mechanických prvkov do objektu organizácie	89
Obr. 49. Diagram hodnotenia nasadenia prvkov poplachového zabezpečovacieho a tiesňového systému	91
Obr. 50. Návrh rozmiestnenia monitorovacieho pracoviska pre jednotlivé mestá	99
Obr. 51. Návrh rozmiestnenia riadiacej pobočky Praha.....	103
Obr. 52. Návrh rozmiestnenia riadiacej pobočky Brno	104
Obr. 53. Návrh pre rozmiestnenie vedúceho riadiaceho pracoviska Olomouc (vľavo: 1PP, vpravo: 1NP).....	107
Obr. 54. Proces preskúmania manažmentom	126

ZOZNAM TABULIEK

<i>Tab. 1. Definovanie základných právnych predpisov o bezpečnostnej politike [18].....</i>	15
<i>Tab. 2. Definovanie vzťahu medzi početnosťou a stupňom poškodenia zdravia [16]</i>	30
<i>Tab. 3. Definovanie kľúčových slov metódy analýzy rizík HAZOP[16]</i>	31
<i>Tab. 4. Kategórie kritickosti metódy analýzy rizík FMEA[16]</i>	32
<i>Tab. 5. Definovanie súčasného počtu zamestnancov na jednotlivých prevádzkach</i>	52
<i>Tab. 6. Všeobecná aplikácia SWOT analýzy do podniku</i>	65
<i>Tab. 7. Bilancia súčasného stavu organizácie.....</i>	66
<i>Tab. 8. Úvodná analýza hrozby zranenia</i>	68
<i>Tab. 9. Vyjadrenie vzťahu medzi kategóriou kritickosti a hodnotou</i>	70
<i>Tab. 10 . Analýza vplyvom porúch a následkov v projekte</i>	71
<i>Tab. 11. Analýza fyzického útoku na objekt</i>	74
<i>Tab. 12. Hodnotenie analýzy príčin následkov.....</i>	74
<i>Tab. 13. Vyhodnotenie hrozby fyzického útoku na organizáciu</i>	75
<i>Tab. 14. Analýza spoľahlivosti zamestnancov</i>	75
<i>Tab. 15. Tabuľkové hodnotenie hodnotiacich pracovných pozícií</i>	76
<i>Tab. 16. Analytické hodnotenie kompetencií obchodného oddelenia</i>	77
<i>Tab. 17. Analytické hodnotenie kompetencií oddelenia bezpečnostného manažmentu</i>	78
<i>Tab. 18. Analytické hodnotenie kompetencií technického oddelenia.....</i>	79
<i>Tab. 19. Analytické hodnotenie kompetencií IT oddelenia</i>	81
<i>Tab. 20. Analytické hodnotenie kompetencií personálneho oddelenia</i>	82
<i>Tab. 21. Vyhodnotenie analytického procesu</i>	85
<i>Tab. 22. Hodnotenie návrhu na zmenu fyzickej bezpečnosti objektu.....</i>	93
<i>Tab. 23. Dokument návrh na zmenu fyzického zabezpečenia objektu.....</i>	94
<i>Tab. 24. Návrh dokumentu Záznam o dokumentácií.....</i>	95
<i>Tab. 25. Hodnotenie pre kontrolu základných funkcií prístupového systému</i>	96
<i>Tab. 26. Návrh definovania priority pre zavedenie prístupového systému</i>	97
<i>Tab. 27. Návrh finálneho hodnotenia splnenia požiadaviek určených smernicou</i>	100
<i>Tab. 28. Návrh úpravy a kategorizácie manipulovaných informácií.....</i>	101
<i>Tab. 29. Návrh prístupových oprávnení pre vstup do miestností monitorovacieho pracoviska</i>	102
<i>Tab. 30. Návrh prístupových oprávnení pre vstup do miestností riadiacej pobočky</i>	105

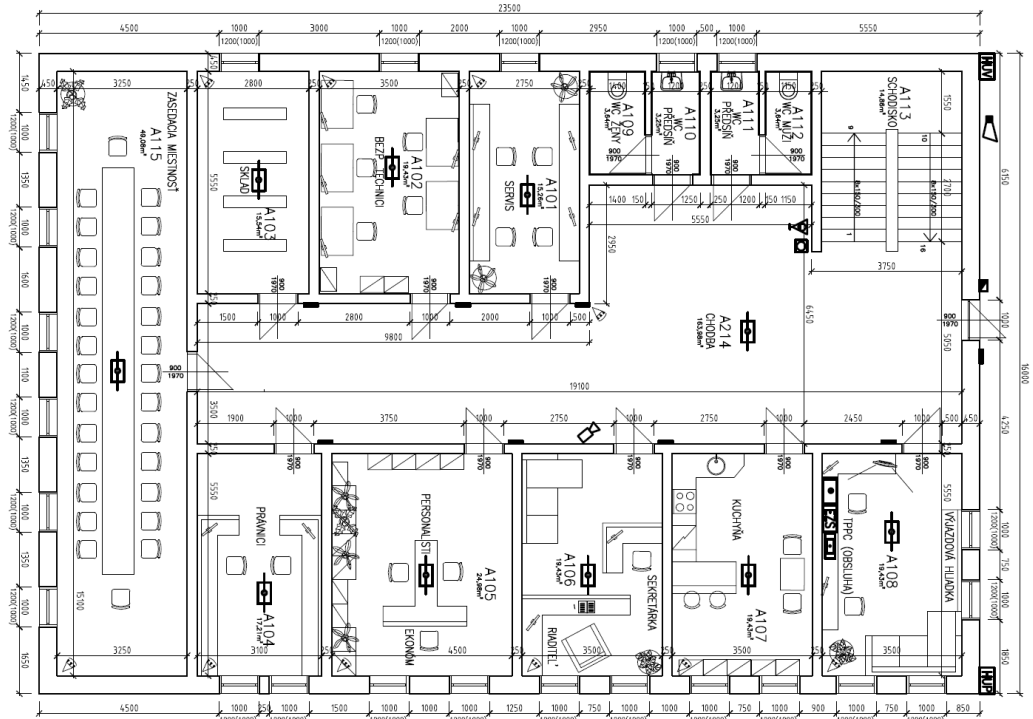
<i>Tab. 31. Návrh prístupových oprávnení pre vstup do miestností vedúcej riadiacej pobočky Olomouc prízemie</i>	108
<i>Tab. 32. Návrh prístupových oprávnení pre vstup do miestností vedúcej riadiacej pobočky Olomouc I. poschodie</i>	109
<i>Tab. 33. Definovanie primárnych dokumentov pre určenie požiadaviek na zamestnancov</i>	110
<i>Tab. 34. Návrh tabuľkového zhodnotenia jednotlivých pracovných požiadaviek.....</i>	111
<i>Tab. 35. Návrh pre definovanie zodpovedných osôb z oblasti BOZP</i>	115
<i>Tab. 36. Definovanie prípadu školenia v oblasti BOZP</i>	116
<i>Tab. 37. Definovanie základnej osnovy v oblasti jednanie taktickej porady BOZP</i>	117
<i>Tab. 38. Definovanie systému školiaceho procesu</i>	117
<i>Tab. 39. Definovanie potreby osobných ochranných a hygienických pomôcok.....</i>	119
<i>Tab. 40. Hodnotiaci zoznam na požiadavky normy ISO 9001 Všeobecné požiadavky</i>	122
<i>Tab. 41. Hodnotiaci zoznam na dokumentáciu ISO 9001 Všeobecné požiadavky</i>	122
<i>Tab. 42. Hodnotiaci kontrolný zoznam na potrebnú dokumentáciu</i>	123
<i>Tab. 43. Definovanie základných zodpovedností</i>	124
<i>Tab. 44. Návrh kontrolného zoznamu pre Záväzok manažmentu</i>	125
<i>Tab. 45. Návrh kontrolného záznamu pre Zameranie na zákazníka</i>	125
<i>Tab. 46. Návrh kontrolného zoznamu dokumentu pre Internú komunikáciu.....</i>	126
<i>Tab. 47. Návrh kontrolného zoznamu na dokumentáciu prípravy zamestnancov</i>	127
<i>Tab. 48. Návrh kontrolného zoznamu pre Realizáciu produktu</i>	128
<i>Tab. 49. Návrh kontrolného zoznamu pre návrh a vývoj produktu/ služby</i>	128
<i>Tab. 50. Návrh kontrolného zoznamu pre proces výberu dodávateľa</i>	129
<i>Tab. 51. Návrh kontrolného zoznamu pre výrobu a poskytovanie služieb</i>	130
<i>Tab. 52. Návrh kontrolného zoznamu pre meranie, analýzy a zlepšovanie</i>	130
<i>Tab. 53. Návrh pre hodnotenie účinnosti jednotlivých bezpečnostných stratégií.....</i>	133
<i>Tab. 54. Návrh časového plánu pre aplikáciu jednotlivých smerníc do procesu</i>	133
<i>Tab. 55. Návrh pre vyhodnotenie.....</i>	134
<i>Tab. 56. Návrh pre definovanie hodnotenia stavu a vyvodenie záveru</i>	134

ZOZNAM PRÍLOH

PRÍLOHA P I: NÁVRH ROZMIESTNENIA KANCELÁRSKYCH PRIESTOROV MINITOROVACÍCH PRACOVÍSK	147
PRÍLOHA P II: NÁVRH ROZMIESTNENIA KANCELÁRSKYCH PRIESTOROV BRNO.....	148
PRÍLOHA P III: NÁVRH ROZMIESTNENIA KANCELÁRSKYCH PRIESTOROV PRAHA	149
PRÍLOHA P IV: NÁVRH ROZMIESTNENIA KANCELÁRSKYCH PRIESTOROV OLOMOUC 1PP	150
PRÍLOHA P V: NÁVRH ROZMIESTNENIA KANCELÁRSKYCH PRIESTOROV OLOMOUC 1NP	151
PRÍLOHA P VI: PRIMÁRNE DEFINOVANIE KOMPETENCIÍ ZAMESTNANECKÝCH FUNKCIÍ.....	152
PRÍLOHA P VII: DEFINOVANIE NAVIAZANOSTI JEDNOTLIVÝCH PROCESOV	153
PRÍLOHA P VIII: NÁVRH ČASOVÉHO PLÁNOVANIA FYZICKEJ OCHRANY	154
PRÍLOHA P IX: ZOBRAZENIA POROVNANIA PROCESU S BEZPEČNOSTNÝMI PRAVIDLAMY A BEZ ICH APLIKÁCIE	155

PRÍLOHA P III: NÁVRH ROZMIESTNENIA KANCELÁRSKÝCH PRIESTOROV PRAHA

PRAHA
Pódorys INP
M1:100



Tabuľka miestnosti

ČÍSLO MENO	PODPA	Podlaha	POČET OSOB
A101	SERVIS	KERAMICKÁ DLAŽBA	4
A102	BEZP. TECHNICI + IT	PLOVOCI PODLAHA	5
A103	SKLAD	KERAMICKÁ DLAŽBA	-
A104	PRÁVNICI	PLOVOCI PODLAHA	2
A105	PERSON. + EKONOM	KERAMICKÁ DLAŽBA	3
A106	RIADITEĽ + SEKRET.	KERAMICKÁ DLAŽBA	2
A107	KUCHYŇA	KERAMICKÁ DLAŽBA	-
A108	TPC OBSLUHA	KERAMICKÁ DLAŽBA	6
A109	WC ŽENY	KERAMICKÁ DLAŽBA	-
A110	PREDSIEŇ ŽENY	KERAMICKÁ DLAŽBA	-
A111	PREDSIEŇ MUŽI	KERAMICKÁ DLAŽBA	-
A112	WC MUŽI	KERAMICKÁ DLAŽBA	-
A113	SCHODISKO	KERAMICKÁ DLAŽBA	-
A114	CHODBA	KERAMICKÁ DLAŽBA	-
A115	ZASIEDACIA MIESTNOSŤ	KERAMICKÁ DLAŽBA	-
UŽITNÁ PLOCHA CELKOM:			317,47

- Pedestrian passage
- PR + antimasking
- Čistka korekt
- Vozňovňa stĺpna s diaľkacm
- Ústredňa EPS
- Ústredňa EZS
- Vydierne kamera
- Testovú tlačtko
- Perový požiarový hadiaci prístroj
- Hlavný úzver plynu
- Hlavný úzver vody
- Kibvennice EZS
- Signálnozné tablo

Svätlá výška 3000 mm
S
10.4.2014

SO01: ±0,000 = 479,30 m.n.m.

ARCHITEKT	ZODP. PROJEKTANTI	PROJEKTANTI	VYTLAČOK Č.
INVESTOR :			
AKCE :		FORMÁT	2x44
		STUPEŇ	
		ARCH. Č.	
DESAH :		DATEM	1.2014
		MERADLO	1:100
		Č. V.	

PRÍLOHA P VI: PRIMÁRNE DEFINOVANIE KOMPETENCIÍ ZAMESTNANECKÝCH FUNKCIÍ

		Definovanie kompetencií							
Oddelenie	Funkcia	vedenie	úroveň vedenia	rozhodovanie	schvaľovanie dok.	vytvorenie projektu	inštalácia	kommunikácia s klientom	
Obchodné oddelenie	obchodný riaditeľ	•	1	•					
	vedúci auditor	•	2	•	•				
	obchodný manažér	•	2		•	•		•	
	obchodný zástupca					•		•	
	interný auditor				•			•	
Oddelenie bezpeč. manaž.	bezpečnostný riaditeľ	•	1	•	•				
	veliteľ vyjazdovej hliadky	•	2	•					
	manažér monitorovacieho centra	•	2		•			•	
	riaditeľ pobočky	•	1	•	•			•	
	obsluha TPPC							•	
	čeln vyjazdovej hliadky							•	
	externý pracovník upratovacej služby								
Personálne oddelenie	personálny manažér			•	•			•	
	personálny zástupca							•	
Technické oddelenie	manažér technického oddelenia	•	1	•	•			•	
	vedúci projektant		3	•	•			•	
	projektant					•		•	
	servisný technik						•	•	
	bezpečnostný technik					•	•	•	
	bezpečnostný konzultant					•	•	•	
IT oddelenie	manažér IT	•	3		•			•	
	IT technik					•	•	•	
Právnické oddelenie	frimenný právnik	•	3		•			•	
Ekonómické oddelenie	ekonom	•	3		•			•	

PRÍLOHA P VII: DEFINOVANIE NAVIAZANOSTI JEDNOTLIVÝCH PROCESOV

Fyzická bezpečnosť		Prístupový systém		Definovanie požiadaviek na zamestnancov a školenia		Tvorba informačného systému
Definovanie záveru		Zostavenie časového plánu pre implementáciu prístupového systému		Zostavenie požiadaviek na výkon pracovnej pozície (kompetencie)		Implementovanie kompetencií do práce s dokumentami
Formulácia problému		Stanovenie kompetencií		Kontrola splnenia požiadaviek na súčasných zamestnancov		Definovanie osôb podieľajúcich sa na jednotlivých projektoch
Návrh riešenia		Kontrola		Definovanie plánu pre doplnenie požadovaných kvalifikácií		
Schválenie riešenia				Definovanie jednotlivých pracovných pozícií (výkon pracovnej úlohy)		Definovanie kontroly
Vymedzenie finančnej čiastky na fyzickú bezpečnosť objektov		Preškolenie zamestnancov		Kontrola aplikovania teoretických poznatkov do procesu		Technické riešenie
Schválenie časového plánu a kompetencií		Zavedenie prístupového systému do prevádzky		Definovanie pravidelných školení		Overenie funkčnosti
Zahájenie projektu				Definovanie sankcií pre neplnenie požiadaviek		
Kontrola činností		Odstránenie nedostatkov a chýb		Kontrola splnenia cieľa		Kontrola splnenia cieľa
Zavedenie systému do prevádzky				<i>Skvalitnenie poskytovaných služieb, zvýšenie odolnosti proti chybe</i>		<i>Riadenie práce s informáciami a projektami</i>
Odstránenie chýb		Kontrola splnenia cieľa				
Kontrola splnenia cieľa		<i>Monitorovanie pohybu osôb po objekte</i>				
<i>Zvýšenie fyzickej bezpečnosti organizácie</i>						
Nastavenie kontroly a aktualizácie plánov						
Zníženie možnosti vzniku nepriaznivej udalosti						

PRÍLOHA P IX: ZOBRAZENIA POROVNANIA PROCESU S BEZPEČNOSTNÝMI PRAVIDLAMI A BEZ ICH APLIKÁCIE

Príkladová štúdia bez implementácie navrhovaných bezpečnostných pravidiel		Prekladová štúdia s implementáciou navrhovaných bezpečnostných pravidiel	
Klient - definovanie potreby	Obchodná stratégia	Klient - definovanie potreby	Obchodná stratégia s bezpečnostnými pravidlami
Obchodný zástupca - návrh riešenia		Návrhové riešenie - technici + obchodný zástupca	
Získanie zákazky		Získanie zákazky	
Návrh technického riešenia		Riadenie projektu	
Zmena návrhu riešenia		Postup podľa projektu	
Možnosť straty zákazníka		Spokojnosť klienta	
Voľný pohyb osôb po objekte	Stratégia prístupu do objektov	Nastavenie prístupových pravidiel	Stratégia prístupu do objektov s bezpečnostnými pravidlami
Vstup neoprávnenej osoby do objektu		Riadený vstup po objektoch	
Únik informácie o organizácii, alebo o klientovi		Monitorovanie pohybu zamestnancov po objektoch	
Strata mena spoločnosti, alebo zákazníka		Riadený prístup návštevy	
		Minimalizovanie možnosti úniku informácií	
Bez organizácie priestorov	Stratégia riadenia	Organizácia priestorov	Stratégia riadenia s bezpečnostnými pravidlami
Pohyb každého zamestnanca je neriadený		Pohyb zamestnanca monitorovaný	
Voľný prístup k citlivým údajom		Definovaný pohyb návštevy	
Únik informácií		Riadenie práce s informáciami - zavedenie informačného systému	
Neurčené pravidlá dokumentácia	Stratégia dokumentácie	Presne definovaná potrebná dokumentácia	Stratégia dokumentácie s bezpečnostnými prvkami
Bez dokumentácie zmien		Definovanie procesov	
Bez špeciálnych postupov		Definovanie pracovných postupov	
Bez vedenia časového plánu		Definovanie kompetencií	
Strata informácií			