

# Zásady a postupy bezpečnostního plánování v privátní praxi

Bc. Tomáš Baťa

---

Diplomová práce  
2014



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

\*\*\*nascannované zadání s. 1\*\*\*

\*\*\*nascannované zadání s. 2\*\*\*

## **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/bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....  
podpis diplomanta

## **ABSTRAKT**

Tato diplomová práce mapuje oblast bezpečnostní expertizy a plánování. Popisuje také související činnosti jako je bezpečnostní analýza a prognóza. Práce zpracovává technologický postup činností s použitím jednotlivých metod. Obsahem je tvorba návrhu bezpečnostního plánování pro konkrétní společnost. V praktické části je uvedena modelová situace, která popisuje jednotlivé části bezpečnostní expertizy. Zde je také vytvořen návrh bezpečnostní politiky organizace. Hlavní částí je podrobný postup bezpečnostního plánování s cílem naplnit požadované podmínky.

Klíčová slova: Bezpečnost, Bezpečnostní plánování, analýza, organizace, bezpečnostní politika

## **ABSTRACT**

This master's thesis maps the area of security expertise and planning. It also describes related activities as security analysis and prognosis. The thesis compiles technological process of activities using particular methods. It consists of a draft of security planning designed for concrete company. The practical section presents a model describing individual parts of security expertise. There is also created a draft of security policy of the organization. Its main part consists of a detailed security planning process in order to fulfill the required conditions.

Keywords: Security, Security planning, Analysis, Organization, Security policy

Děkuji panu JUDr. Štefkovi za jeho trpělivost, ochotu a spolupráci po celou dobu mého studia. Moje velké díky patří též celé rodině za lásku, podporu a motivaci.

Tato práce je věnována mému tatínkovi, který v minulém roce zemřel.

Motto:

*„Když všichni mluví o nemožnostech, hledej možnosti!“*

Tomáš Baťa (1876 – 1932)

# OBSAH

<b>ÚVOD</b> .....	<b>11</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>12</b>
<b>1 BEZPEČNOSTNÍ EXPERTIZA</b> .....	<b>13</b>
1.1 ÚVOD DO PROBLEMATIKY BEZPEČNOSTI.....	13
1.2 VÝCHOZÍ BODY PRO ZPRACOVÁNÍ BEZPEČNOSTNÍ EXPERTIZY .....	15
1.2.1 Cíle bezpečnostní expertizy .....	16
<b>2 BEZPEČNOSTNÍ PLÁNOVÁNÍ</b> .....	<b>17</b>
2.1 PROCES PLÁNOVÁNÍ .....	17
2.1.1 Úloha plánování .....	17
2.1.2 Sestavování plánu .....	19
2.2 METODY V BEZPEČNOSTNÍM PLÁNOVÁNÍ .....	22
2.2.1 Ganttův diagram .....	22
2.2.2 Síťový graf .....	22
2.2.3 PERT diagram .....	23
2.3 ZÁSADY BEZPEČNOSTNÍHO PLÁNOVÁNÍ.....	23
2.4 PRŮBĚH BEZPEČNOSTNÍHO PLÁNOVÁNÍ .....	25
2.5 VÝSLEDEK BEZPEČNOSTNÍHO PLÁNOVÁNÍ .....	25
2.5.1 Projekt zabezpečení ochrany bezpečnostních zájmů firmy .....	25
2.5.2 Projekt optimalizace ochrany bezpečnostních zájmů firmy .....	27
2.6 PROCES BEZPEČNOSTNÍHO PLÁNOVÁNÍ.....	28
2.7 SEGMENTY V BEZPEČNOSTNÍM PLÁNOVÁNÍ A ŘÍZENÍ .....	31
2.7.1 Posloupnost a vypracování dle systémového přístupu .....	31
<b>3 BEZPEČNOSTNÍ ANALÝZA</b> .....	<b>33</b>
3.1 ANALÝZA SWOT .....	34
3.2 ANALÝZA PEST.....	37
3.3 PARETOVA ANALÝZA.....	39
3.3.1 Krizová matice .....	41
3.4 ANALÝZA STROMEM PORUCH FTA.....	42
3.5 ANALÝZA STROMEM UDÁLOSTÍ ETA .....	43
3.6 ANALÝZA PŘÍČIN A NÁSLEDKŮ CCA.....	45
3.7 IŠIKAVŮV DIAGRAM .....	45
3.7.1 Rozdělení do kategorií.....	46
3.7.2 Výhody diagramu .....	48
<b>4 BEZPEČNOSTNÍ PROGNÓZA</b> .....	<b>49</b>
4.1 CÍLE BEZPEČNOSTNÍ PROGNÓZY .....	49
4.2 POUŽITÍ BEZPEČNOSTNÍ PROGNÓZY .....	49
4.2.1 Kvantitativní a kvalitativní přístup .....	50
4.3 ROZDĚLENÍ METOD.....	50
4.3.1 Osobní hodnocení.....	50
4.3.2 Panelová shoda .....	51
4.3.3 Metoda Delphi .....	51

4.3.4	Metoda klouzavých průměrů.....	51
4.3.5	Metoda exponenciálního vyrovnání .....	52
4.3.6	Prognostické modely .....	52
4.4	VYHODNOCENÍ PROGNÓZY .....	53
<b>5</b>	<b>HODNOCENÍ RIZIK .....</b>	<b>55</b>
5.1	AKTIVUM.....	55
5.2	ZDROJ HROZBY.....	55
5.3	HROZBA (NEBEZPEČÍ) .....	55
5.3.1	Klasifikace hrozeb .....	55
5.4	RIZIKO .....	56
5.5	ZRANITELNOST .....	57
5.6	BEZPEČNOSTNÍ OPATŘENÍ.....	57
5.7	ŘÍZENÍ RIZIK .....	58
<b>6</b>	<b>BEZPEČNOSTNÍ POLITIKA ORGANIZACE.....</b>	<b>59</b>
6.1	PODMÍNKY BEZPEČNOSTNÍ POLITIKY .....	59
6.2	KLASIFIKACE .....	60
6.3	PŘÍSTUPY K ŘEŠENÍ OTÁZKY BEZPEČNOSTNÍ POLITIKY .....	62
6.3.1	Krátká politika .....	62
6.3.2	Rozsáhlá politika .....	62
6.4	PROBLÉMY PŘI TVORBĚ POLITIKY.....	63
6.5	SHRNUTÍ BEZPEČNOSTNÍ POLITIKY JAKO PROSTŘEDKU BEZPEČNOSTNÍHO PLÁNOVÁNÍ.....	63
6.6	BEZPEČNOSTNÍ POLITIKA INFORMAČNÍCH SYSTÉMŮ.....	64
6.6.1	Cíle bezpečnostní politiky organizace .....	66
6.6.2	Kritéria bezpečnostní politiky informačních systémů .....	67
6.6.3	Analýza rizik informačních systémů .....	67
<b>7</b>	<b>BEZPEČNOSTNĚ TECHNICKÉ POŽADAVKY NA BEZPEČNOST ORGANIZACE .....</b>	<b>70</b>
7.1	TERMÍNY A TERMINOLOGIE.....	70
7.2	ZÁSADY SYSTÉMU VNITŘNÍHO ŘÍZENÍ BEZPEČNOSTI PODNIKU A PRVKY TOHOTO SYSTÉMU .....	72
7.3	ÚKOLY VEDENÍ PODNIKU PŘI ZAVÁDĚNÍ SYSTÉMU VNITŘNÍHO ŘÍZENÍ BEZPEČNOSTI .....	74
7.3.1	Koordinace činností na všech stupních řízení včetně koordinace dodavatelské činnosti.....	75
7.3.2	Kontrolní činnosti a audit.....	76
7.3.3	Rozsah vnitřní kontroly na pracovišti.....	77
<b>II</b>	<b>PRAKTICKÁ ČÁST .....</b>	<b>81</b>
<b>8</b>	<b>ZAVEDNÍ BEZPEČNOSTNÍ POLITIKY ORGANIZACE .....</b>	<b>82</b>
8.1	PROFIL SPOLEČNOSTI.....	82
8.2	STRUKTURA SPOLEČNOSTI.....	83
8.2.1	Vedení společnosti.....	83
8.2.2	Bezpečnostní management.....	84
8.2.3	Oddělení nákupu.....	84

8.2.4	Obchodní oddělení.....	85
8.2.5	Oddělení informačních systémů.....	85
8.2.6	Oddělení logistiky .....	85
8.2.7	Finanční a právní oddělení.....	85
8.3	<b>STRUKTURA BEZPEČNOSTNÍ POLITIKY ORGANIZACE .....</b>	<b>86</b>
8.3.1	Obecná ustanovení.....	86
8.3.2	Oblast personální bezpečnosti.....	86
8.3.3	Oblast organizační.....	89
8.3.4	Oblast informačních systémů.....	90
8.3.5	Oblast ochrany majetku .....	93
8.3.6	Oblast bezpečnostní a status bezpečnostního managementu.....	95
<b>9</b>	<b>ZPRACOVÁNÍ BEZPEČNOSTNÍHO PLÁNU ORGANIZACE K ZAVEDENÍ TECHNICKÝCH A TECHNOLOGICKÝCH PROSTŘEDKŮ BEZPEČNOSTI PRO NOVÝ SKLAD SPOLEČNOSTI.....</b>	<b>98</b>
9.1	<b>ANALÝZA .....</b>	<b>98</b>
9.1.1	Úvaha o přístupu k řešení úkolu.....	98
9.1.2	Benchmarking jako metoda k řízení bezpečnosti v organizaci.....	99
9.1.2.1	Výhody benchmarkingu.....	100
9.1.3	Sběr informací.....	101
9.1.4	Třídění a výběr informací .....	103
9.1.5	Studium a rozbor .....	105
9.1.5.1	Metody sběru dat:.....	106
9.1.6	Zobecnění.....	106
9.2	<b>ROZHODOVÁNÍ .....</b>	<b>106</b>
9.2.1	Ujasnění problému.....	106
9.2.2	Zpracování variant postupu řízení.....	107
9.2.2.1	Varianta 1.....	107
9.2.2.2	Varianta 2.....	107
9.2.2.3	Varianta 3.....	108
9.2.2.4	Varianta 4.....	108
9.2.3	Volba optimální varianty a formulace rozhodnutí.....	108
9.3	<b>PLÁNOVÁNÍ .....</b>	<b>109</b>
9.3.1	Určení omezujících podmínek .....	109
9.3.2	Formulace základních předpovědí.....	109
9.3.2.1	Bezpečnostní posouzení objektu .....	109
9.3.3	Stanovení konkrétních úkolů.....	112
9.3.4	Určení prostředků činnosti.....	112
9.3.5	Vypracování plánu postupu řízení.....	113
9.4	<b>PLÁN OCHRANY OBJEKTU .....</b>	<b>113</b>
9.4.1	Režimová opatření.....	113
9.4.1.1	Kontrola vstupu do objektu skladu.....	113
9.4.1.2	Pohyb v prostorech skladu .....	113
9.4.1.3	Pravidla pro řidiče externích společností.....	114
9.4.1.4	Kontrola příjmu zboží.....	115
9.4.1.5	Kontrola výdeje zboží.....	116
9.4.1.6	Speciální režimová oprávnění skladu.....	116
9.4.2	Fyzická ochrana.....	117
9.4.2.1	Pravidla pro výkon strážní služby .....	117

9.4.2.2	Harmonogram fyzické ochrany objektu .....	119
9.4.3	Technická ochrana .....	120
9.4.3.1	Elektrický zabezpečovací systém (PZTS) .....	120
9.4.3.2	Požární bezpečnost .....	123
9.4.3.3	System CCTV .....	123
9.4.3.4	Přístupové systémy .....	125
9.4.3.5	Napojení na dohledové a poplachové přijímací centrum.....	125
9.4.4	Plán krizové připravenosti .....	126
9.4.4.1	ZÁKLADNÍ ČÁST .....	126
9.4.4.2	OPERATIVNÍ ČÁST .....	127
9.4.4.3	POMOCNÁ ČÁST .....	128
9.4.5	Zpracování typových plánů .....	128
9.5	ORGANIZOVÁNÍ ČINNOSTÍ .....	129
9.5.1	Motivování a stimulování .....	129
9.5.2	Koordinování a operativní řízení.....	129
9.6	HODNOCENÍ VÝSLEDKŮ .....	130
9.6.1	Zjišťování fakt.....	130
9.6.2	Kritické posouzení.....	130
9.6.3	Návrh opatření.....	130
9.6.4	Uplatnění zkušeností z praxe .....	130
9.7	PLÁNOVACÍ SOFTWARE JAKO NÁSTROJ PRO ŘÍZENÍ PROJEKTU ....	131
9.8	KONTROLNÍ SEZNAM A PŘÍSTUPY K JEHO VYUŽITÍ BEZPEČNOSTNÍM MANAGEMENTEM.....	132
9.9	NEUSTÁLÝ ROZVOJ A ZPĚTNÁ VAZBA .....	133
<b>ZÁVĚR</b> .....		<b>135</b>
<b>SEZNAM POUŽITÉ LITERATURY</b> .....		<b>136</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK</b> .....		<b>140</b>
<b>SEZNAM OBRÁZKŮ</b> .....		<b>142</b>
<b>SEZNAM TABULEK</b> .....		<b>143</b>
<b>SEZNAM PŘÍLOH</b> .....		<b>144</b>

## ÚVOD

Bezpečnostní plánování - jako jedna z forem činností průmyslu komerční bezpečnosti - je velmi podstatné pro zavedení komplexního systému zabezpečení. Ctí základní pravidlo, jakým je ochrana lidského života, zdraví, majetku a životního prostředí. Je zde velmi důležité dodržet postup a zahrnout všechny podmínky, které budou tento systém podporovat. Podstatou je tedy koordinace úkolů v oblasti průmyslu komerční bezpečnosti a osob uvnitř tohoto systému, jejímž cílem je zajištění bezpečného prostředí. Nedílnou součástí procesu plánování je zpracování analýz a prognóz, které nám pomohou poodkrýt důvody zabezpečení a předpovědět jejich správnou funkci v rodícím se procesu. Důležitou součástí fungování bezpečnosti v oblasti privátní praxe je stanovení bezpečnostní politiky organizace. Popisuje jasný rámec, na jehož základech budeme moci vystavět náš systém. Činnost bezpečnostního managementu bude v tomto směru klíčová, bude celý systém plánování řídit a zároveň za celý proces zodpovídat. V praktické části bude uvedena situace, před kterou stojí organizace z oblasti privátní praxe. Tento postup vytvoří tým bezpečnostního managementu. Jejím úkolem je zhodnotit bezpečnostní rizika organizace a zhotovit bezpečnostní plán, dle všech známých postupů. Praktická část je psána pohledem bezpečnostního manažera, pracujícího pro zmíněnou organizaci s cílem vytvoření technologického prostupu zabezpečení. Tento postup je zpracován v podobě seznamu kroků pro splnění cíle bezpečnostního plánování. Uvedené postupy jsou provedeny v písemné i grafické formě. Příklady grafických výstupů bezpečnostního plánování zpracovaných softwarem Microsoft Project 2013 jsou součástí příloh.

## **I. TEORETICKÁ ČÁST**

# 1 BEZPEČNOSTNÍ EXPERTIZA

## 1.1 Úvod do problematiky bezpečnosti

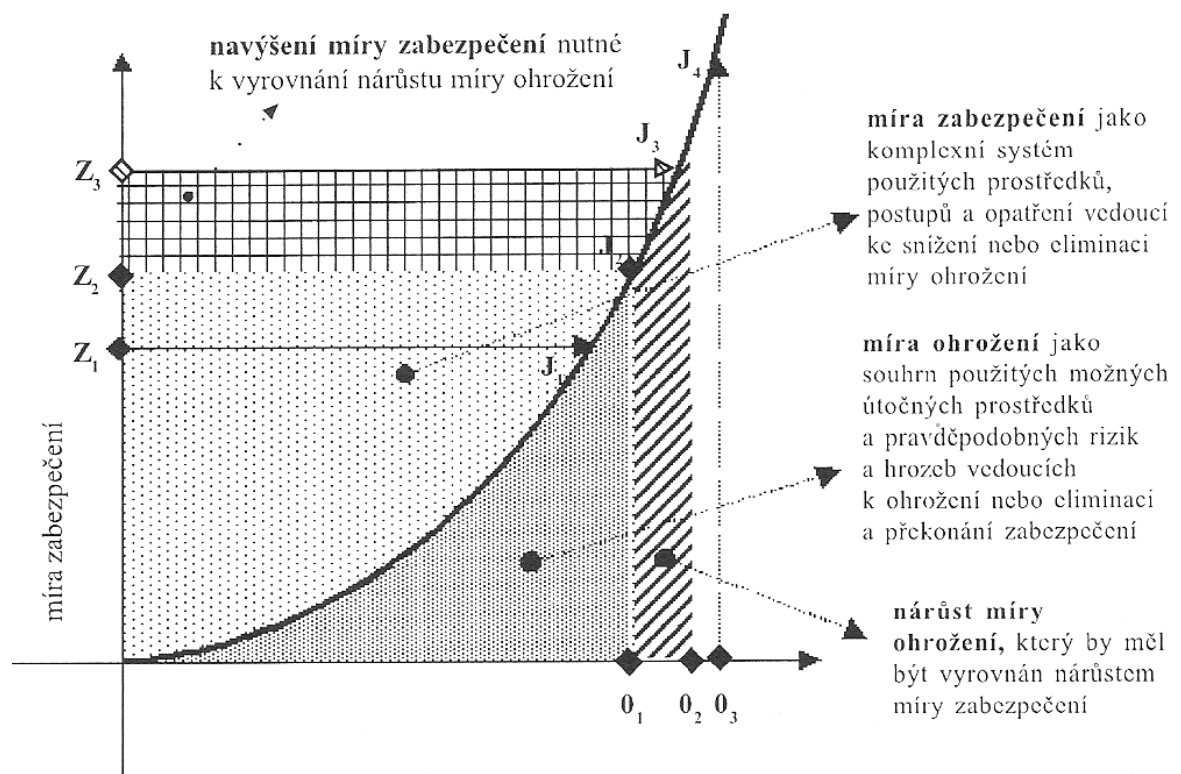
Problematiku zabezpečení řeší lidstvo již od nepaměti. V průběhu času tato problematika vykryštovala do třech velkých skupin:

- Vše, co je spojeno s podstatou lidské existence, tj. zdraví a život.
- Vše, co je spojeno s vlastnickými vztahy k hmotným věcem a k majetkovým právům, tj. materiální existence.
- Vše, co je spojeno s pozorováním a ochranou zájmů jednotlivých osob, tj. společenské existence.

Narušení kterékoli z nich může vést k narušení ostatních dvou skupin. Pokud následek může mít řadu příčin, tak i příčina může vyvolat řadu následků. Lidstvo používá prostředky zabezpečení od nepaměti, postupem času se ale mění technologie zabezpečení. Princip ochrany vlastnictví však zůstává v nezměněné podobě, liší se pouze vylepšenými metodami zabezpečení, které již byly dávno objeveny. Kdokoli se kdy snažil vědomě něco ochránit, resp. zabezpečit před možným nebezpečím, činil tak na základě jisté úrovně poznání. Jeho poznání určitých skutečností mu po čase umožnilo definovat:

- Cíl zabezpečení (ve smyslu dosažení žádaného stavu – jistoty).
- Objekt zabezpečení (život, zdraví, vlastnická práva).
- Způsob a prostředky zabezpečení.
- Materiálové i finanční náklady na zabezpečení.
- Termíny, do kdy je zabezpečení nutné realizovat.
- Osoby, které za zabezpečení nesou osobní odpovědnost.

Úroveň, účinnost, použité prostředky a náklady na zabezpečení jsou přímou reflexí míry nebezpečí, nebo ohrožení. Mezi těmito dvěma pojmy existuje vztah závislosti. [3]

Obr. 1 Vztah míry zabezpečení na míře ohrožení<sup>1</sup>

Pozn.  $Z_{1,2}$  stupeň (míra) zabezpečení

$O_{1,2,3}$  stupeň (míra) ohrožení

$J_{1,2,3,4}$  stupeň (míra) jistoty

Na grafu vidíme vzájemný vztah míry ohrožení a míry zabezpečení, dále také vidíme, že když míra ohrožení vzroste, je nutné, aby vzrostla i míra zabezpečení, jinak se účinnost zabezpečení sníží, nebo znehodnotí – dojde ke ztrátě jistoty. Žádoucí stav je rovnováha mezi mírou ohrožení a mírou zabezpečení (v grafu průsečík obou úseček na křivce). Nedsahuje-li míra zabezpečení míry ohrožení, je celý tento systém zabezpečení poddimenzovaný a nemůže dostatečně plnit svou roli – neeliminuje možné nebezpečí. Graficky je tato situace znázorněna např. jako vztah mezi mírou zabezpečení  $Z_3$  a mírou ohrožení  $O_3$ , kdy výsledkem je míra jistoty  $J_4$ . Pro matematické vyjádření platí, že rozdíl mezi  $Z_3$  a  $O_3$  je zá-

<sup>1</sup> Převzato z: BRABEC, František a kolektiv. *Bezpečnost pro firmu, úřad, občana*, Praha, Public History, 2001, ISBN 80-86445-04-6.

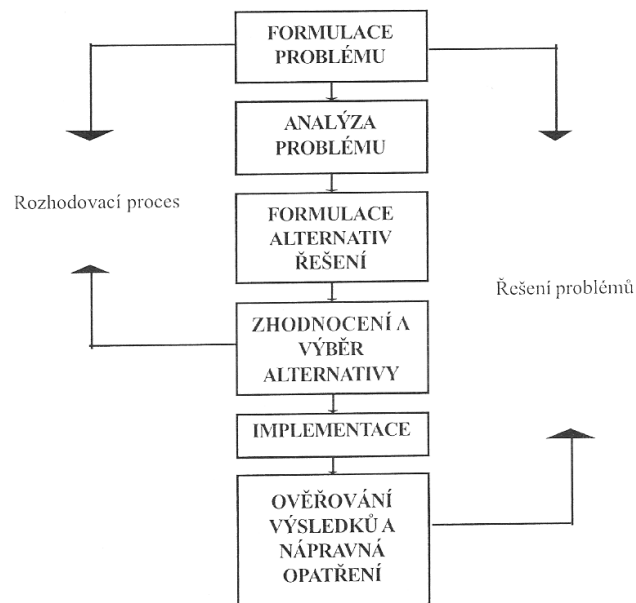
pornou hodnotou, neboť  $o_3 > z_3$ . Stav, kterého chceme při zabezpečení dosáhnout, by se vyjádřil jako rozdíl mezi  $z$  a  $o$ , kdy se rovná nule, nebo je větší než nula. ( $z - o > 0$ ) V grafu tento stav je patrný na vztahu mezi  $z_2$  a  $o_1$ , případně  $z_3$  a  $o_2$  (vyrovnaný stav), nebo mezi  $z_3$  a  $o_1$  (míra zabezpečení převyšuje míru ohrožení).

Pojem bezpečnost – bezpečnostní opatření charakterizujeme jako systém. Právě tato vlastnost je určující i pro přístup k řešení problémů spojených s bezpečností. Tento přístup musí být zásadně systémový. Základní informace pro bezpečnostní expertizu organizace nejsou v podobě přesných čísel, což samozřejmě omezuje možnost výběru a použití různých technik analýzy a prognózy.

Zabezpečení organizace tvoří systém opatření, jehož cílem je, aby organizace jako celek i její jednotlivé organizační složky a její zaměstnanci byli chráněni před vnějšími i vnitřními vlivy, které by jí mohly způsobit ztráty na zdraví a životě, škody na majetku, nebo poškodit její oprávněné cíle a zájmy spjaté s existencí a činností organizace v procesu hospodářské soutěže. [3]

## 1.2 Výchozí body pro zpracování bezpečnostní expertizy

K zajištění bezpečnosti organizace musíme provést řadu kroků, které jsou předem dány a jejichž pořadí je určeno. V počátku řešení problému je nezbytné problém zformulovat. Následuje analýza problému, výsledkem této analýzy bude určení možností k řešení problému, přesněji řečeno formulace alternativ řešení. Následující fáze je velmi důležitá, protože v ní dochází k posouzení jednotlivých alternativ řešení a k výběru jedné z alternativ. K dalšímu kroku pro vyřešení problému je implementace rozhodnutí. Proces bezpečnostní expertizy by měl vždy obsahovat zpětnou vazbu, tj. ověřování výsledků rozhodnutí a přijetí nápravných opatření.

Obr. 2 Proces zpracování bezpečnostní expertizy<sup>2</sup>

Bezpečnostní expertizu můžeme dělit na dva způsoby a to na dílčí bezpečnostní expertizu, nebo komplexní bezpečnostní expertizu. Pro oba způsoby však platí, že jde o postup prováděný odborníky v průmyslu komerční bezpečnosti, který mapuje současný stav a poté navrhuje příslušná opatření. Součástí bezpečnostní expertizy tedy budou všechny tyto velké skupiny, mezi které patří bezpečnostní analýza, prognóza a bezpečnostní plánování.

### 1.2.1 Cíle bezpečnostní expertizy

Cílem komplexní bezpečnostní expertizy organizace je zjistit aktuální stav zabezpečení a dále navrhnout prostředky a opatření k účinnému řešení optimalizace bezpečnostního problému organizace. Je třeba respektovat celkový strategický plán firmy a její cíle s ohledem na organizační, personální a ekonomické možnosti. [3]

<sup>2</sup> Převzato z: BRABEC, František a kolektiv. *Bezpečnost pro firmu, úřad, občana*, Praha, Public History, 2001, ISBN 80-86445-04-6.

## 2 BEZPEČNOSTNÍ PLÁNOVÁNÍ

Podstatou bezpečnostního plánování v průmyslu komerční bezpečnosti je vytvoření vědecky odůvodněného programu činnosti systémů aparátů průmyslu komerční bezpečnosti v zájmu dosažení stanoveného cíle.

Veškeré metody a postupy směřují k dokončení rozhodovacího procesu v oblasti komplexní bezpečnostní expertízy, tj. k sestavení komplexního bezpečnostního plánu organizace a jeho podrobného rozpracování do podoby bezpečnostního projektu. Rozsah, složitost přípravy a sestavení projektu jsou přímo závislé na velikosti a složitosti plánovaného cíle. Zabýváme se otázkou komplexního zabezpečení organizace, jde nám tedy především o komplexní bezpečnostní projekt, který bude zahrnovat řadu dílčích cílů. K jeho dokončení bude potřeba více zúčastněných, v rámci něho bude řešeno více úkolů a některé i souběžně, což si žádá vysoké nároky na koordinaci jednotlivých činností. Bezpečnostní plán (projekt) charakterizuje jeden významný znak, kterým je dosažení určeného cíle. V okamžiku dosažení cíle plán (projekt) končí. Bezpečnostní projekty podobně jako ostatní druhy projektů se vyznačují některými charakteristickými rysy, jedná se zpravidla o tyto hlavní znaky:

- Projekty mají přesně srozumitelné a definované cíle.
- Projekty obsahují jednoznačné termíny dokončení.
- Obsahují množinu činností propojenou vzájemnými vazbami.
- Pro jejich realizaci jsou vyčleněny materiální a lidské zdroje (v podobě rozpočtu).
- Obsahují seznamy pracovníků odpovědných za realizování projektu.
- Realizují je zpravidla projektové týmy (jejich splnění nelze zajistit jediným člověkem).

### 2.1 Proces plánování

#### 2.1.1 Úloha plánování

- Zabezpečení výběru a stanovení cílů.
- S pomocí plánování vyhledáváme účinnější cesty a způsoby dosažení těchto cílů.
- S pomocí plánu určujeme potřebné množství sil a prostředků k jejich dosažení a také se určují způsoby optimálního rozmístění sil a prostředků.

- S pomocí plánu se zabezpečuje koordinovanost všech článků a prvků systému průmyslu komerční bezpečnosti. [12]

Na počátku realizace projektu stojí otázka definování cíle projektu – je to naprosto nezbytná podmínka každého plánu. Pokud není cíl definován, nemáme co plánovat. Cíl musí být určen a také vyjádřen jednoznačně a srozumitelně. Jednoznačně ve smyslu, že jej nelze zaměnit za cíl jiný a srozumitelně v tom smyslu, že každý, kdo se na přípravě plánu a jeho realizaci bude podílet, mu porozumí. Projekt musí být také měřitelný – jen tehdy, jestliže jej lze kvalifikovat (např. provést montáž 7 kamer v objektu A), případně je možné dosáhnout pouze dvou stavů ano / ne, cíl splněn / cíl nesplněn. Formulace by neměla být příliš obecná, například, že jde o zvýšení celkové bezpečnosti organizace. Tato formulace neobsahuje dostatek informací, které by byly vodítkem při vypracování projektu. Jde o proklamaci bez závaznosti, nikoli plánovaný cíl. Cíl by měl být definován přesněji např. cílem projektu je komplexní zabezpečení organizace a to v oblasti informační, technické, objektové, administrativní a personální v souladu s požadavky zákona o utajovaných skutečnostech. Takto definovaný cíl je určitý a srozumitelný pro všechny zúčastněné pracovníky. Jde v něm o to, aby organizace po stránce bezpečnostní splnila podmínky, požadující zákon č. 148/1998 Sb., o ochraně utajovaných skutečností. Formulace plánovaného cíle je však i výsledkem předchozí činnosti organizace, resp. provedení bezpečnostní expertizy.

Na začátku všeho existuje problém v bezpečnostní oblasti, který chce organizace řešit. Důvody pro to mohou být různé, je však důležité, že organizace formulovala problém a hodlá jej řešit. Problémem může být např. skutečnosti, že se organizace chce zúčastňovat výběrových řízení a získávat důležité státní zakázky, kde však je ze zákona určena podmínka, že organizace musí mít potvrzení NBÚ o bezpečnostní prověrce. Organizace je tedy postavena před problém. Výstupem rozhodnutí bude to, že vyřeší problém buď vlastními silami, či celou věc, nebo její určitou fázi přenechá k řešení dodavatelské odborné firmě. V tomto případě nám pomůže podrobení problému analýze a syntéze, po kterých získáme určitou úroveň a prohloubíme poznání problému. Výsledkem tohoto poznávacího procesu bude zjištění současného stavu úrovně zabezpečení ve vztahu k již formulovanému problému. Na základě toho příslušní odborníci vypracují řešení problému a to obvykle ve více variantách. Současně upřesní původní formulaci problému, protože ta se pod vlivem získaných poznatků může pozměnit. Například vyjde najevo, že po stránce technického zabezpečení je organizace zabezpečena v souladu s požadavky zákona, ale režimová opatření nejsou dostatečná a nejsou ani dodržována. Na základě provedené bezpečnostní analýzy jsou od-

kryty nedostatky, které úkol upřesní a musí být vyřešeny. V našem příkladě bychom tedy hovořili o splnění podmínek příslušného zákona v oblasti režimových opatření. Formy a způsoby řešení těchto zjištěných nedostatků se promítnou do existence více navrhovaných variantních řešení. Na základě předložených variant zpravidla vrcholové vedení organizace po jejich prostudování rozhodne, kterou z alternativ zrealizuje. Vybrané řešení je pak odrazovým můstkem pro konečné, přesné a srozumitelné zformulování plánovaného cíle. Výsledkem pro formulování cíle plánu jsou tedy závěry provedené bezpečnostní expertizy, abychom byli přesnější, bezpečnostní analýzy. Kromě bezpečnostní analýzy má na konečnou podobu cíle projektu významný vliv i bezpečnostní prognózování a bezpečnostní politika organizace.

Nesmíme zaměňovat pojmy alternativa řešení problému s alternativami plánu (projektu), jedná se o dvě odlišné věci. Jednotlivé varianty řešení bezpečnostního problému nám umožňují vybrat takové řešení samotného problému, které je vzhledem k možnostem a potřebám organizace nejvhodnější. Varianty bezpečnostního plánu nám umožňují vybrat nejoptimálnější jednotlivé činnosti a postupy při realizaci již zvolené varianty řešení bezpečnostního problému. Varianty plánu se mohou stanovovat i pro případ, že by původní plán nemohl být realizován z neočekávaných důvodů v té podobě, v jaké byl přijat. Důvodem může být například zdržení technologických dodávek ze strany dodavatele atd.

Termín dokončení je další významnou součástí projektu. Abychom mohli sestavit plán, je potřeba vědět, kdy má být plánovaného cíle dosaženo. Termín dokončení je jedním z limitujících faktorů plánu vymezující časový prostor, v němž bude muset být provedena řada kroků nutných k dosažení plánovaného cíle. V některých případech mohou být organizace tlačeny při sestavování bezpečnostního projektu pevně stanoveným termínem ze zákona, v jiných případech závazný termín vyplyne například z požadavku zadavatele veřejné zakázky, nebo z termínu jiného projektu, který je bezpečnostnímu projektu nadřazen. K určení celkového termínu splnění plánu je velmi důležité, v jakých termínech je možné realizovat jednotlivé dílčí kroky, jenž musí být nezbytně provedeny, aby plánovaného cíle bylo dosaženo.

### **2.1.2 Sestavování plánu**

Při sestavování plánu je velmi důležité definovat správně množinu všech činností, resp. úkolů, které je nutné pro splnění plánovaného cíle provést a určit vazby mezi nimi. Definujeme všechny kroky, které povedou ke splnění plánu. Tyto úkoly determinují rozsah pro-

jektu. Nejdříve je nutné určit hlavní části projektu, a když jsou určeny, lze se na ně zaměřit jednotlivě. Následně se zaměříme na výběr dodavatele technologií, apod. Pokud určíme všechny jednotlivé úkoly, zjistíme, že je důležitá časová posloupnost provádění těchto úkolů. Musíme tedy vypracovat určitou hierarchii stanovených úkolů. Zjistíme tím, které úkoly lze provádět souběžně a které musí být prováděny za sebou. Odkryjí se nám tím časové vazby mezi jednotlivými úkoly. Důležité je také určit dobu trvání jednotlivých úkonů, protože to má samozřejmě vliv na celkovou dobu trvání realizace projektu a tedy i na celkový termín dokončení. Zjistili jsme tedy, že některé úkoly mohou být prováděny paralelně a některé v časové návaznosti. Je tedy zřejmé, že celková doba realizace projektu není dána prostým součtem dob trvání všech nutných úkolů. Kromě časových vazeb mezi jednotlivými úkoly existují tedy ještě i vzájemné závislosti, které určují, zda úkol může být proveden nezávisle na provedení jiného úkolu, či naopak může být zahájen a proveden jen tehdy, jestliže mu předchází dokončení jiného úkolu. V průběhu projektu existují určité body, které nazýváme milníky. Jsou to události, nebo podmínky, kdy je ukončena celá skupina k sobě se vztahujících úkolů, nebo určitá fáze projektu. Milníky nám pomáhají organizovat úkoly do logických celků.[17]

Aby plán mohl být úspěšný, musí být kromě určení jednotlivých kroků k jeho dosažení zabezpečen i materiálně – musí být tedy definovány zdroje projektu. Zdroje jsou lidé, vybavení a prostory. Zdroje jsou zpravidla vyjádřeny ve formě rozpočtu. Ne všechny zdroje však musí mít bezprostředně vliv na výši rozpočtu, zvláště bude-li organizace k realizaci všech, nebo některých úkolů využívat vlastní zdroje, může se tímto finanční rozpočet projektu snížit. Pokud se budeme bavit o lidech jako o jednom ze zdrojů projektu, musí být známo ještě před započítáním projektu, kolik osob jakých profesí se realizace zúčastní a zda jde o pracovníky organizace, nebo o externí pracovníky a dodavatele. V této fázi není nutné určovat konkrétní jména. Dále je důležité, zda se jednotliví pracovníci budou po dobu plnění úkolu v rámci projektu věnovat i jiné činnosti s projektem nesouvisející, v případě, že ano, ve kterých termínech mohou být na práci v rámci projektu použiti. Pro vybavení, které je dalším zdrojem projektu, platí obdobné požadavky. Určíme tedy, jaké vybavení projektu potřebujeme (počítače, vozidla) - zda budou z vlastních zdrojů organizace, nebo od dodavatelů a konečně, kdy a na jak dlouhou dobu příslušné vybavení potřebujeme. Prostory jsou též velmi významným zdrojem plánu, zejména prostory nutné k uskladnění technologie, nebo strojů a zařízení, prostory pro provoz po dobu realizace plánu. Zpravidla se jedná o zdroje vlastní, ale nemusí tomu tak být vždy (uskladnění je řešeno pronajmutím

externího skladu). Jestliže některé dílčí úkoly plánu pro organizaci provádí jiné organizace nebo jednotlivci dodavatelským způsobem (na klíč), je otázka zajištění zdrojů pro tento úkol ponechána na příslušném dodavateli. Pro úspěšnost projektu je nutné určit konkrétní osoby odpovědné za splnění jednotlivých dílčích úkolů a celého plánu. Na provedení jednotlivých úkolů bezpečnostního projektu se může podílet řada pracovníků organizace i externích pracovníků a dodavatelů. Jejich činnost je třeba navzájem koordinovat a je nutné zajistit výměnu potřebných informací mezi nimi. Manažer projektu (nazývajícím se také správce projektu) je odpovědný za jeho realizaci a musí být schopen plnit následující úkoly:

- Kontrolovat, zda jsou jednotlivé fáze plněny včas.
- Včas rozpoznat možnost vzniku problému a přijmout příslušná opatření k eliminaci negativních dopadů na plnění plánu.
- Zajistit a využívat vhodný monitorovací systém, který mu umožní vyhodnotit stav plnění postupu projektu.
- Rychle a přesně reagovat na odchylky od předpokládaného průběhu plánu (přijímat včas adekvátní opatření).
- Přesně plánovat požadavky na omezené zdroje tak, aby byly v souladu s plánovaným průběhem projektových prací.
- Rozlišovat priority jednotlivých úkolů z hlediska jejich nároků na omezené zdroje.

Pro správce projektu je důležité, aby dokončil projekt v požadovaném termínu, nepřekročil rozpočet a splnil požadované cíle. Tento požadavek je oprávněný a vyplývá z přijatého plánu. Tyto požadavky musí být splněny všechny současně, nikoliv jeden z nich na úkor jiného. Správce projektu odpovídá za konečnou realizaci – splnění konečného cíle, vedle něj pracují ještě subdodavatelé, odpovědní za provedení jednotlivých dílčích úkolů. Správce projektu se nemůže hájit tím, že někdo další úkol nesplnil. V případě problému je správný postup takový, že správce vidí problém, musí najít nová řešení a provést nutné změny tak, aby bylo dosaženo cíle. V rámci realizace rozsáhlých bezpečnostních projektů své místo nachází i tzv. projektové týmy. Jedná se tedy o organizace, které svou velikostí, počtem zaměstnanců a charakterem i významem své podnikatelské činnosti - při řešení otázek komplexního zabezpečení - budou realizovat řadu náročných a nákladných úkolů. Jde zejména o velké průmyslové závody, holdingy, banky apod. Jeden člověk, nebo malá

skupina v tomto případě není schopna zajistit požadovanou práci a pro tyto případy jsou zakládány projektové týmy. [17]

## 2.2 Metody v bezpečnostním plánování

V souvislosti s plánováním a projektováním, je třeba upozornit na skutečnost, že management podniku má k dispozici řadu softwarových produktů pro PC, usnadňující proces plánování. Mnoho z nich umí sestavit komplexní strategický plán celé organizace. Vytvářejí určité modely možných budoucích podmínek a prověřují, zda plán i za těchto podmínek obstojí – výstupem tedy bude komplexní podnikatelský plán. Takové produkty tedy můžeme s úspěchem použít i při sestavování bezpečnostního plánu organizace. Projektování má vypracované své techniky, které můžeme s úspěchem aplikovat i na bezpečnostní projektování. Hovoříme o technikách pomáhajících při organizaci projektu a při jeho realizaci:

- Ganttův diagram
- Síťový diagram a jeho nástavba diagram PERT
- Metoda kritické cesty

Veškeré uvedené techniky jsou použitelné i při řízení bezpečnostního projektu.

### 2.2.1 Ganttův diagram

Ve svém principu se jedná o velmi jednoduchou a účinnou metodu. Diagram zobrazuje souhrn jednotlivých činností, dobu potřebnou k jejich provedení a vzájemné časové vazby mezi nimi. Každý úkol v tomto diagramu je vyznačen jako vodorovný proužek. Jednotlivé úkoly jsou zobrazeny pod sebou a mezi nimi jsou tvořeny grafickým způsobem vazby, které ukazují, že příkladně určitý úkol nelze začít dříve, než skončí úkol jiný atd. Všechny úkoly v podobě proužků jsou umístěny pod vodorovnou časovou stupnicí, ze které můžeme snadno odečíst, kdy konkrétní úkol má začít a kdy skončí, resp. do kdy nejpozději má být proveden. Diagram je vhodnější používat na zobrazení délky trvání jednotlivých činností a celého projektu než na vyjádření vzájemných vazeb. Jedná se o výborný kontrolní nástroj na zjištění stavu jednotlivých úkolů v čase.

### 2.2.2 Síťový graf

Obsahuje veškeré potřebné informace pro řízení realizace projektu. Typickými prvky síťového grafu jsou uzly a jejich spojnice. Každý uzel v podobě malého kroužku reprezentuje

časový bod – zahájení, nebo ukončení činnosti. Činnost je vyjádřena úsečkou – spojnicí, která oba uzly spojuje. Při vynášení síťového grafu je nutné se držet určitých obecných pravidel:

- Graf musí mít jeden počáteční a jeden koncový uzel.
- Každému uzlu (s výjimkou výchozího) musí předcházet minimálně jedna činnost.
- Po každém uzlu (s výjimkou koncového) musí následovat minimálně jedna činnost.
- Kterékoli dva uzly smí spojovat pouze jedna činnost.

Při kreslení grafu je nutné dodržovat určité konvence platné pro zobrazování. Například, že počáteční a koncový uzel se nezobrazují jako kroužky, ale jako kosočtverce apod. Síťový graf je pro využití řízení projektu využitelný tehdy, jestliže obsahuje, kromě již zmíněného úplného výčtu činností (úkolů), časové informace, nejdříve možná ukončení činností, nejpozději nutná ukončení všech činností a identifikovanou kritickou cestu síťového grafu.

### 2.2.3 PERT diagram

Jedná se o variantu síťového grafu. Na rozdíl od běžného síťového grafu, vyžadujícího striktně propojení všech úkolů mezi sebou i za cenu použití nulové délky činností (tzv. činnost fiktivní), PERT diagram nemusí zobrazovat vazby sumárních úkolů na dílčí úkoly.

Kritický úkol je takový, který je kritický z hlediska dokončení celého projektu. Jinými slovy takový, jehož zdržení ohrozí splnění celého projektu v plánovaném termínu. Z pohledu doby provádění činností jsou nekritické úkoly ty, které mají určitou časovou rezervu a kritické ty, které žádnou časovou rezervu nemají. Kritická cesta začíná u počátečního uzlu a končí u uzlu konečného. Její délka je rovna součtu dob trvání kritických úkolů a udává celkovou délku realizace projektu. Metoda kritické cesty je standard při správě projektu pro zjištění kritických úkolů. Základem je matematický model zohledňující vztahy mezi úkoly, dobu jejich trvání a veškerá omezení týkající se dostupnosti jejich zdrojů. Metoda se používá především pro stanovení počátečního a konečného data jednotlivých úkolů. Tuto metodu vyvinula v 50. letech společnost DuPont Corporation & Remington Rand.

## 2.3 Zásady bezpečnostního plánování

- **Úplnost a provázání bezpečnostních opatření** - jednotlivá plánovaná opatření buď v podobě návrhu optimalizace, nebo projektu musí na sebe navzájem navazovat a musí se též vzájemně prolínat.

- **Přiměřenost bezpečnostních opatření** - realizujeme jen taková bezpečnostní opatření, která jsou přiměřená jak z hlediska bezpečnostních cílů, tak i z pohledu přípustných hranic svépomoci a v mezích nutné obrany a krajní nouze<sup>3</sup>. Bezpečnostní opatření musí být v souladu s bezpečnostními cíli.
- **Akceschopnost bezpečnostních opatření** – plánovaná i prováděná bezpečnostní opatření musí být způsobilá k realizaci a způsobilá k rizikům a škodám, nebo tato rizika a škody musí být schopná minimalizovat. Vyžadujeme těmito bezpečnostními opatřeními dosažení žádoucího stavu v naplnění bezpečnostních cílů a musí předpokládat nebezpečí situací, jimiž by mohla být jednotlivá bezpečnostní opatření ztížena, nebo zcela znemožněna.
- **Praktičnost bezpečnostních opatření** – bezpečnost není podnikatelským cílem, ale jedním z prostředků ke zdárné realizaci komplexu podnikatelských cílů příslušné firmy.
- **Komplexnost bezpečnostních opatření** – Bezpečnostní opatření musí být navržena tak, aby zamezovala celkovému ohrožení bezpečnosti v příslušné firmě. Nelze se tedy soustředit na pouhé odstranění, nebo snížení nebezpečí jednotlivých rizik či škod, ale na bezpečnostní ochranu je nutno přihlížet jako na komplex.
- **Variantní přístup k bezpečnostnímu plánování** – Bezpečnostní plánování by mělo být vyhotoveno v několika variantách. Hlediskem pro tvorbu variant může být komfortnost zajištění bezpečnostních zájmů, poměr mezi fyzickou ochranou, technickou ochranou a tzv. vnitřní ochranou, atd. U jednotlivých variant je nutné stanovit klady a zápory i jaký stupeň rizik jednotlivé varianty připouštějí. Zadavatel rozhodne, která varianta bude vybrána, žádná varianta však nesmí připouštět nadměrná

---

<sup>3</sup> Krajní nouze dle § 28 trestního zákoníku - "čin jinak trestný, kterým někdo odvrací **nebezpečí** přímo hrozící zájmu chráněnému tímto zákonem, není trestným činem."

Nutná obrana dle § 29 trestního zákoníku - "čin jinak trestný, kterým někdo odvrací přímo hrozící nebo trvajícím **útok** na zájem chráněný tímto zákonem, není trestným činem. Nejde o nutnou obranu, byla-li obrana zcela zjevně nepřiměřená způsobu útoku." [18]

rizika. Komfort ochrany bezpečnostních zájmů se odráží v nákladech na realizaci bezpečnostních opatření při jejich realizaci.

## 2.4 Průběh bezpečnostního plánování

Bezpečnostní plánování probíhá na bázi dílčích bezpečnostních analýz, z nich vycházejících dílčích bezpečnostních prognóz, bezpečnostních koncepcí a jejich syntézou v celkovou bezpečnostní koncepci zajištění firemní bezpečnosti. Při celkovém projektu naplnění bezpečnostních zájmů a cílů firmy se vychází z rozvíjení dílčích cílů. Rámcové pojetí dílčích cílů vychází z kritérií:

- **Místa a nebezpečí rizik** – budovy, provozy, jednotlivé obory činnosti – komodity, místnosti, prostory.
- **Času nebezpečí vzniku rizik** – doba provozu objektů (budov, zařízení), denní, či noční doba, roční doba, atd.
- **Procesu nebezpečí rizik** – náplně jednotlivých funkčních míst, probíhajících činností, probíhajících technologických procesů, apod.
- **Organizace nebezpečí rizik** - struktury, ohraničení odpovědnosti, formálních, či neformálních skupin, apod.

## 2.5 Výsledek bezpečnostního plánování

Výsledkem bezpečnostního plánování bude vypracování projektu zabezpečení ochrany bezpečnostních zájmů firmy, návrh optimalizace ochrany bezpečnostních zájmů firmy a projektu optimalizace ochrany bezpečnostních zájmů firmy.

### 2.5.1 Projekt zabezpečení ochrany bezpečnostních zájmů firmy

Podstatou tohoto projektu bude vypracování komplexu opatření k zajištění ochrany a os-  
trahy bezpečnostních zájmů v objektech, kde ještě tato opatření nejsou uplatňována. Naším cílem bude vypracování nového systému bezpečnostních opatření. Projekt zahrnuje:

- Vlastní zpracování systému bezpečnostních opatření.
- Vypracování řádu (statutu) výkonu služby (realizace bezpečnostních opatření).
- Vypracování směrnic výkonu služby pro jednotlivé konkrétní objekty, nebo činnosti.

- Vypracování typových plánů opatření (na jednotlivé potencionálně možné mimořádné události).
- Vypracování systému režimových opatření.
- Vypracování projektů stavebně technických úprav a montáže technických zabezpečovacích systémů apod.

### **Návrh optimalizace ochrany bezpečnostních zájmů firmy**

Podstatou tohoto návrhu je variantní zpracování návrhů na zajištění ochrany. Návrhy optimalizace by měly směřovat k:

- optimalizační změně systému bezpečnostních opatření,
- optimalizační změně dokumentů sloužících pro realizaci bezpečnostních opatření,
- optimalizační změně stávajících a doplnění chybějících typových plánů opatření,
- požadavkům na personální zajištění,
- požadavkům na finanční zajištění a k ekonomickým rozvahám,
- optimalizačním změnám stávajících, či doplnění chybějících organizačních a režimových opatření,
- požadavkům na stavebně technické úpravy,
- požadavkům na montáž technických zabezpečovacích systémů, apod.

Vše výše uvedené s propočtem odhadu<sup>4</sup> nákladů jak provozních, tak investičních, či jiného materiálního zabezpečení akce. Při smluvním způsobu realizace jednotlivých dílčích opatření, či celého komplexu bezpečnostních opatření se uplatnění tohoto aspektu mimo jiné stává základem pro stanovení ceny služeb. Tato situace bude platit i pro případy další optimalizace (dopracování, úpravy, či přepracování) tudíž je nutné vytvořit rezervu, pro případ dalších nákladů s tím spojených.

---

<sup>4</sup> Ekonomickou rozvahou

### 2.5.2 Projekt optimalizace ochrany bezpečnostních zájmů firmy

Podstatou projektu je vypracování plánu systému bezpečnostních opatření na podkladě vybraných dílčích variant, či komplexní varianty optimálního zabezpečení. Rozdíl mezi projektem zabezpečení a projektem optimalizace se nachází v tom, že v prvním případě hovoříme o novém vypracování, zatímco v druhém pojmu mluvíme o systémové změně. Ať kvalitativní, či kvantitativní, případně obojí stávajícího systému bezpečnostních opatření.

Projekt optimalizace zahrnuje:

- Dopracování, či přepracování systému bezpečnostních opatření zadavatelem již přijatých a schválených variant návrhu optimalizace opatření.
- Dopracování, či přepracování řádu výkonu služby (realizace bezpečnostních opatření) zadavatelem již přijatých a schválených variant návrhu optimalizace opatření. Součástí řádu výkonu služby by měly být i obecné pracovní náplně pro jednotlivé skupiny funkčních míst tzv. firemní bezpečnosti - zajišťovaných vlastními pracovníky firmy, nebo zabezpečovaných dodavatelsky na smluvním základě.
- Zpracování chybějících, dopracování, nebo přepracování stávajících směrnic výkonu služby pro jednotlivé konkrétní objekty, případně činnosti zadavatelem již přijatých a schválených variant návrhu optimalizace opatření. Součástí směrnic výkonu služby budou i konkretizované pracovní náplně pro funkční místa zabezpečující systém bezpečnostních opatření u konkrétního objektu. Tyto zmíněné pracovní náplně musí být konkretizovány pro jednotlivá pevná, nebo pochůzková strážní stanoviště, pro konkrétní činnost, vnitřní ochrana firmy – vnitřní vztahy, vnější ochrana firmy – vnější vztahy, apod.
- Vypracování chybějících, přepracování, nebo dopracování stávajících typových plánů opatření na jednotlivé možné mimořádné události.
- Vypracování projektů stavebně technických úprav a montáže technických zabezpečovacích systémů je záležitostí stavebního, strojírenského, či elektrotechnického projektování. V rámci bezpečnostního poradenství (i v rámci bezpečnostní analýzy a bezpečnostního plánování) půjde v tomto směru o návrh variant řešení a výběr optimální varianty a zadání projektu odbornému pracovišti příslušného oboru.

## 2.6 Proces bezpečnostního plánování

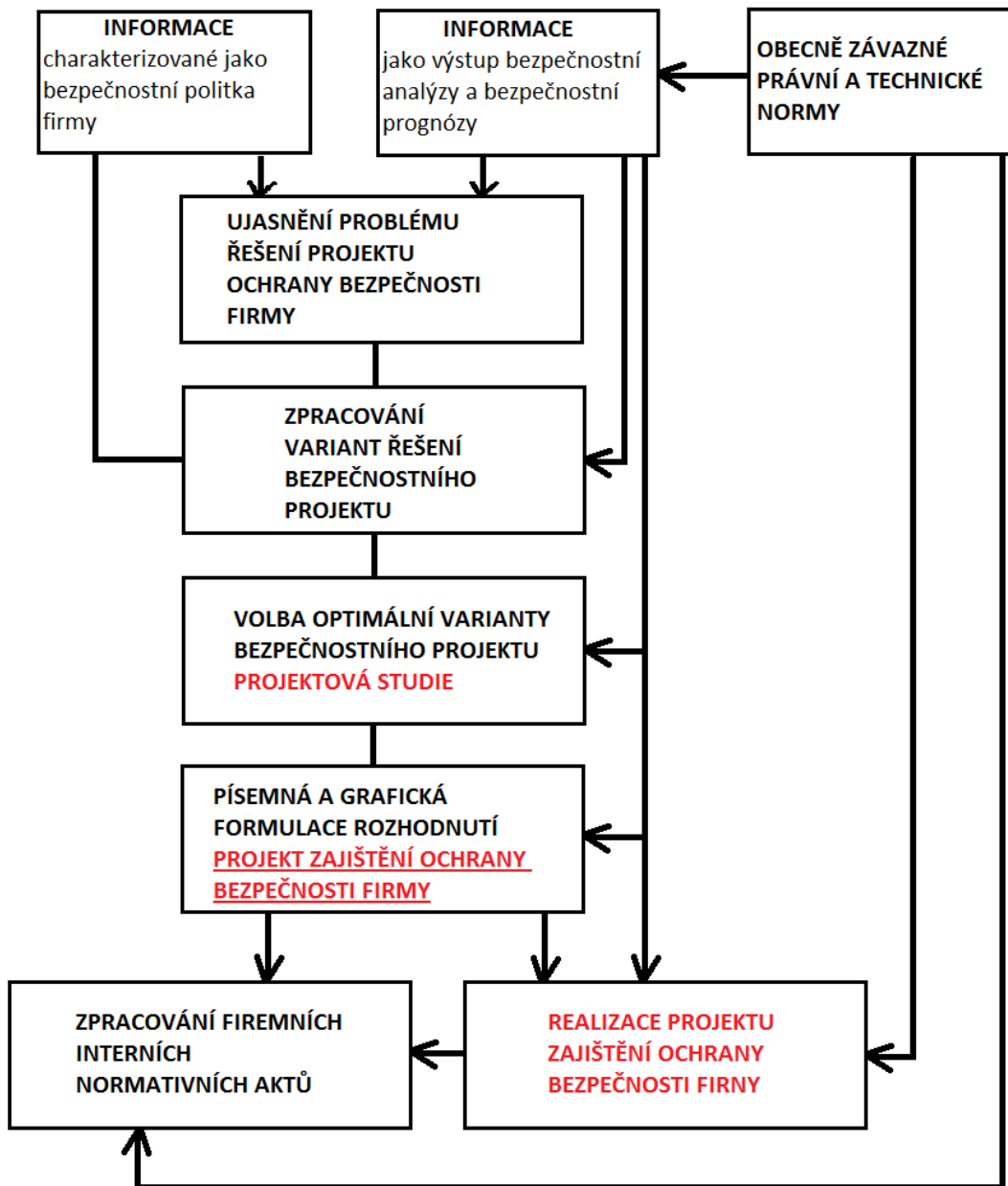
Proces bezpečnostního plánování<sup>5</sup> je charakterizován jako specifická forma rozhodovacího procesu. Tento proces bezpečnostního plánování je představován rozhodovacím procesem, který obsahuje následující parametry:

- **Informační vstupy** – zde použijeme výstupy bezpečnostní analýzy, bezpečnostní prognózy a koncepci představovanou bezpečnostní politikou firmy.
- **Ujasnění problému**
  - Spolehlivost a všestrannost předpovědi (prognózy).
  - Možnost zajištění ochrany bezpečnosti firmy.
  - Nabídka alternativních možností a příležitostí zajištění bezpečnosti firmy.
  - Dosavadní zkušenosti s podobným problémem.
  - Vymezení kritérií pro hodnocení variant, apod.
- **Zpracování variant řešení projektu** – provádíme postupem tzv. hlavních článků, které v žádné z variant nemohou být opomenuty. V jednotlivých variantách jsou poté odlišně řešeny tzv. vedlejšími články, jejichž výběr může být různý a fakticky jimi naplňujeme stupeň komfortu zajištění ochrany bezpečnosti firmy. Vycházíme z dostupných informací, závažnosti, složitosti problému a kritérií jeho řešení, časového hlediska, apod.
- **Volba optimální varianty projektu**
  - Reálnost řešení v jednotlivých variantách.
  - Rizikovost při uplatnění konkrétní varianty.
  - Posouzení účinnosti a efektivnosti jednotlivých variant.
  - Časové a věcné spojitosti s dřívějšími rozhodnutími.
  - Dodržování zákonnosti.
  - Posouzení materiální a finanční náročnosti určité varianty.

---

<sup>5</sup> Plánování = projektování

- Celkové posouzení předností a nedostatků varianty ve vztahu k řešenému problému.
- Výběr optimální varianty z hlediska stanovení kritérií. [3]
- **Formulace rozhodnutí** – do písemné a grafické podoby. Rozhodnutí ztvárněné v projektu ochrany bezpečnosti firmy musí být:
  - Přesné, nerozporné, jasné a úplné.
  - S ohledem na účel relativně stručné, ale přitom srozumitelné, vykonatelné, konkrétní a adresné.
  - Rozhodnutí by mělo řešit formy, metody a prostředky zajištění ochrany bezpečnosti firmy.
  - Mohou být zformulovány i motivační faktory.
  - Stanovena odpovědnost za realizaci jednotlivých opatření.
  - Formulovány způsoby a postupy organizace, řízení, koordinace, součinnosti a spolupráce a také kontroly. [2]

Obr. 3 Proces bezpečnostního plánování<sup>6</sup>

<sup>6</sup> Převzato z: BRABEC, František. *Ochrana bezpečnosti podniku*, EUROUNION, s.r.o., Praha 1996, ISBN 80-85858-29-0.

## 2.7 Segmenty v bezpečnostním plánování a řízení

### 2.7.1 Posloupnost a vypracování dle systémového přístupu

Bezpečnostní analýzu a bezpečnostní plánování je zapotřebí považovat za nezastupitelný prvek efektivnosti realizace bezpečnostních opatření směřujících k zajištění tzv. podnikové bezpečnosti. Tuto podnikovou bezpečnost je třeba chránit jako komplex<sup>7</sup> a účinné zabezpečení podnikové bezpečnosti je možné při řádném fungování celého komplexu bezpečnostních opatření. Pojmem systémový přístup rozumíme řešení problému systémovým pohledem, umožňujícím vidět výsledný systém jako jednotu prvků a vazeb mezi nimi.

a. **Formulace úkolu řízení** – vytyčení problému řízení

b. **Analýza**

- Úvaha o přístupu k řešení úkolu
- Sběr informací
- Třídění a výběr informací
- Studium a rozbor
- Zobecnění

c. **Rozhodování** (jak řešit?)

- Ujasnění problému
- Vypracování variant řešení postupu řízení
- Volba optimální varianty
- Formulace rozhodnutí

d. **Plánování** (kdo, co, kdy, kde?)

- Určení omezujících podmínek
- Formulace základní předpovědi

---

<sup>7</sup> Systém složený z řady subsystémů

- Stanovení konkrétních úkolů
- Určení prostředků a činností
- Vypracování plánu postupu řízení

**e. Organizování činnosti**

- Motivování
- Stimulování
- Koordinování
- Operativní řízení – regulování

**f. Hodnocení výsledků**

- Zjišťování fakt
- Kritické posouzení
- Návrh opatření
- Uplatnění zkušeností z praxe

Mezi každou fází a v průběhu každé fáze cyklu řízení probíhá kontrola, která může vést k:

- Korigování – korekce informace pro další fázi.
- Započetí zcela nového cyklu řízení. [2]

### 3 BEZPEČNOSTNÍ ANALÝZA

Nasbírané a seříděné informace zpracujeme procesem analýzy. Bezpečnostní analýzu můžeme charakterizovat jako metodu poznání, kde podstatou je postupné rozdělení celku na jednotlivé části, studium těchto částí a jejich vzájemných vztahů. Jde o poznávací metodu, ve které postupujeme od obecného ke konkrétnímu. Obecný pohled na problematiku poskytuje obecné poznatky a zkoumaný objekt nám začleňuje do okolního prostředí a vypovídá především o jeho vnějších vazbách, postupnou změnou ohniska pohledu pronikáme pod povrch zkoumaného objektu a poodhalují se nám skutečnosti na první pohled neviditelné. Jedná se o části celku a vzájemné vazby mezi nimi - často i netušené zákonitosti a mechanismy jejich fungování, či selhávání. Abychom dospěli k cíli a smyslu analýzy, nemůžeme se zastavit u jednoduchého členění celku na části a soustředění se na detail. Je nezbytné odhalit tyto vzájemné vztahy mezi danými částmi, mechanismy a zákonitostmi jejich vzájemného fungování. Proces, jímž toto dokážeme, se nazývá syntéza.

Při tvorbě tohoto procesu skládáme jednotlivé části zpátky do celku, musíme však pochopit jednotlivé vazby - mezi celkem a jeho částmi. V okamžiku správně provedené syntézy jsme schopni odpovědět na otázky typu: proč nějaký proces funguje tak, jak funguje; proč daná činnost byla úspěšná, nebo neúspěšná, zda bezpečnostní opatření jsou schopna splnit úkoly, které jsou na ně kladeny, atd. Analýza i syntéza jsou spolu úzce spjaty, na první pohled působí protikladně, existuje však mezi nimi harmonický soulad. V lidském podvědomí jsou často spojovány jako jedna metoda současně. Pokud budeme nadále hovořit o analýze, bezpečnostní analýze, budeme mít vždy na mysli i následné použití metody druhé - syntézy.

Bezpečnostní analýza musí respektovat zákonitosti vědeckého poznávání a odpovědět nejprve na otázky:

- Proč analyzujeme? K zamezení ztrát a jejich minimalizaci.
- Kdy analyzujeme? V okamžiku, kdy nebezpečí hrozí přerůst v hrozbu.
- Co analyzujeme? Lidské zdroje, procesy, majetek, stav zabezpečení.
- Čím analyzujeme? Nástroji analýzy. [13]

Nezapomínáme na základní kriminalistické otázky: kdo, co, kdy, kde, jak, čím a proč? Analýza i syntéza je základní metoda, která nám pomůže poznat a popsat fungování jevů a událostí. Jedná se o metodu, která je pro lidské vědomí vrozená a kterou i často bezděčně

na velmi jednoduché úrovni provádíme. Analytický přístup ke zkoumání dané problematiky jsou spojeny s otázkami:

Proč a jak nastaly důsledky, které nastaly?

Proč věc funguje tak, jak funguje?

Jak postupovat, aby důsledky byly jiné, než byly doposud? [9]

Pro bezpečnostní analýzu organizace platí vše, co o analýze bylo řečeno. Název nám napoví, jaké je její zaměření. Analýza podrobuje zkoumání předměty, jevy, informace a skutečnosti - týkající se přímo, či nepřímo bezpečnosti organizace. Dále jejího bezpečnostního systému s cílem přispět k nalezení přiměřených bezpečnostních prostředků a opatření, které se hodí k řešení bezpečnostního problému organizace. Bezpečnostní analýza je vymezovaná tím, kdo bezpečnostní analýzu požaduje a určeným cílem, kterého má být analýzou dosaženo. Při bezpečnostní analýze provádíme sběr, třídění a slučování informací, které jsou relevantní formulovanému bezpečnostnímu problému organizace a jejímu vytčenému bezpečnostnímu cíli. Je důležité, aby bezpečnostní analýza dokázala postihnout veškeré vazby mezi bezpečnostní problematikou organizace a organizací jako celkem. Záleží též velmi na šíři formulovaného problému, a zda je bezpečnostní analýza prováděna v rámci komplexní bezpečnostní expertizy, nebo jen v rámci dílčí bezpečnostní expertizy. Velmi propracovaným a specifickým druhem bezpečnostní analýzy je bezpečnostní analýza informačních systémů.

V případě bezpečnostní analýzy nebyly zpracovány žádné obecně platné postupy a techniky, nebo mezinárodní standardy. Lze však k vlastnímu provádění analýzy využít řady metod a technik z jiných oblastí, jde především o oblast ekonomiky a financí. Analytické metody a techniky jsou zpravidla managementu organizace známy, což má pro nás určitou výhodu. Pomáhá překonávat počáteční nedůvěru k odbornosti prováděné bezpečnostní expertizy ze strany odpovědných pracovníků organizace. Mezi techniky použitelné k provádění bezpečnostní analýzy organizace můžeme zařadit např.: analýzu SWOT, analýzu PEST, Paretovu analýzu, Išikavův diagram, modifikovanou analýzu stupně ohrožení (vč. znázornění v krizové matici) atd.

### 3.1 Analýza SWOT

Jedná se o analýzu používanou řadou organizací při formulování strategického plánu organizace. Dle názvu, který je akronymem odvozeným z prvních písmen anglických slov

Strengths (přednosti – silné stránky), Weakness (nedostatky – slabé stránky), Opportunities (příležitosti) a Threats (hrozby), obsahuje informaci o tom, co bude předmětem analyzování. Analýza vychází z úvahy, že cesta k dosažení strategického úspěchu organizace je závislá na maximalizaci jejích předností a příležitostí na minimalizaci jejích nedostatků a hrozeb. Pro účely bezpečnostní analýzy je nutno tuto metodu modifikovat. Předmětem analýzy nebude celá organizace a její postavení na trhu, pouze stav její bezpečnosti jako celku. Mezi **přednosti** mohou patřit vnitřní podmínky v organizaci - jako je například dobře propracovaná struktura organizace, přesné rozdělení kompetencí a pravomocí mezi jednotlivé řídicí pracovníky, odborná kvalifikace pracovníků působících v oblasti bezpečnostní organizace, nebo mající vliv na bezprostřední fungování této organizace. V neposlední řadě také dobré finanční zdroje, atd. Mezi **nedostatky** organizace mohou patřit nepříznivé vnitřní podmínky v organizaci, mající negativní vliv na její bezpečnost. Jedná se například o nedostatečně rozvinutou a definovanou organizační strukturu, špatnou ekonomickou a finanční situaci, nepřátelsky naladěný management, který bezpečnostní expertizu a analýzu chce, ale jen proto, že musí, nedůvěřuje odborníkům, protože na to má své lidi, je to moc drahé atd. Dále mezi nedostatky může patřit absence kvalifikovaných pracovníků v oblasti zabezpečení, nebo jejich nedostatek, nekvalitní nebo vůbec žádná zabezpečovací technika, nevýhodná lokalizace organizace, či objekty, které mají být zabezpečeny, atd.

**Příležitostmi** rozumíme podmínky, které příznivě ovlivňují organizaci v jejím postavení na trhu jak v současnosti, tak i v budoucnu. Pokud tyto příležitosti mohou příznivě ovlivňovat a zasahovat organizaci jak v současnosti, tak v budoucnu, jsou pro nás použitelné a důležité. Jde například o zvýšení konkurenceschopnosti a následně zlepšené finanční a ekonomické situace, generující finanční zdroje, které jsme schopni v rámci organizace investovat do zlepšení bezpečnostních opatření, atd. Svou roli zde sehrávají i změny zákonů, které mohou ovlivnit účast organizace na výběrových řízeních o významné zakázky tím, že nastaví příznivější parametry její účasti v takovém řízení. Mezi parametry může patřit změna podmínek pro úroveň vnitřních bezpečnostních opatření v organizaci. Mezi příležitostmi můžeme zařadit dlouhodobé snížení cen bezpečnostních zařízení a služeb v důsledku příznivého vývoje vnějších ekonomických vztahů, apod.

**Hrozby** mají nepříznivý dopad na stav zabezpečení organizace z pohledu negativních podmínek vnějšího prostředí, jak v současnosti, tak i v budoucnu. Zasahují, nebo mohou zasáhnout organizaci jako celek a jejich negativní dopad na zabezpečení organizace je až

druhotný. Může se však jednat o hrozby, které zasáhnou bezpečnostní opatření organizace přímo. Jako příklad nám může sloužit, změna zákona, která zpřísní podmínky pro zabezpečení organizace. Pro organizaci to představuje vynaložení větších finančních prostředků - například pro dosažení bezpečnostních standardů, které jsou podmíněny při výběrovém řízení na získání zakázky. Obecnou hrozbou s důsledky na chod celé organizace, může být ztráta jedné nebo více významných zakázek a tím snížení ekonomických výsledků a pokles finančních zdrojů. Další nepříznivý vliv na bezpečnost organizace má také zvýšení kvantitativní a kvalitativní úrovně zabezpečení konkurenčních organizací, důvodem je zaostávání z pohledu bezpečnosti za těmito společnostmi. Mezi přednostmi, nedostatky, příležitostmi a hrozbami nalezneme takové podmínky, které ovlivňují stav a úroveň zabezpečení v organizaci buď bezprostředně, nebo zprostředkovaně. Některé z těchto podmínek vytvářejí tlak na rychlou a zásadní změnu bezpečnostních opatření v organizaci, jinde je vidět potřeba výhledová při pohledu do budoucna. [1]

Po dokončení této analýzy jsou schopni - analytik s vedoucími pracovníky - objektivně posoudit současný stav bezpečnosti organizace a zavést opatření, která umožní organizaci udržet, nebo zvýšit kvalitativní i kvantitativní úroveň zabezpečení i v budoucnu. Do této chvíle hovoříme o jedné analýze, ve skutečnosti, však jde o analýzy čtyři. Pro větší přehlednost analýzy a dosažení výsledku přeneseme informace do grafické podoby kříže, který plochu rozdělí do čtyř kvadrantů. Kvadrant I. znázorňuje oblast, v níž se uplatňuje soulad externích příležitostí a interních předností. Kvadrant II. pak oblast, kde nelze využít externích příležitostí z důvodů interních nedostatků. Kvadrant III. ukazuje situaci, kdy externí hrozba ohrožuje existenci organizace z důvodů jejích interních nedostatků a konečně kvadrant IV. ilustruje situaci, kdy může být poškozena vnitřní organizační přednost v důsledku vnější hrozby. [3]

Obr. 4 Diagram analýzy SWOT <sup>8</sup>

Mezi výhody analýzy SWOT patří schopnost hodnocení současného i budoucího stavu, což zjednodušuje a zpřesňuje volbu nejvhodnějších účinných opatření. Přispívá ke zlepšení fungování systému bezpečnosti organizace za předpokladu, že bezpečnostní pracovníci dovedou správně identifikovat a pochopit význam vnitřních nedostatků a vnějších hrozeb. Tuto analýzu je možné často opakovat, může být tady často aktualizována a tak může odrážet změny ve vnitřních a vnějších podmínkách, zejména ve smyslu zabezpečení organizace. [1]

### 3.2 Analýza PEST

Podobně jako analýza SWOT získala svůj název složením čtyř počátečních písmen slov, která charakterizují předmět její analýzy. Jde o Politiku, Ekonomiku, Sociální oblast a Technologii – právě na tyto oblasti je zkoumání zaměřeno. Analýza událostí a trendů může právě v těchto oblastech vedení společnosti přinést informace o okolním prostředí v širším záběru včetně pravděpodobných budoucích trendů. Aplikací této metody na bezpečnost organizace musíme zúžit záběr zkoumání pouze na ty události a trendy v uvedených oblastech, které mají, nebo mohou mít význam pro zabezpečení organizace.

Pro odborné firmy podnikající v bezpečnostním průmyslu, by měla být tato metoda metodou základní, která jim umožňuje orientovat se v dané problematice. Neměla by být vytvářena jen pro určitou zakázku, ale trvale na obecné úrovni. Znalost událostí a trendů v jednotlivých oblastech – mající vliv na bezpečnost organizace – je totiž podmínkou

<sup>8</sup> Převzato z: BRABEC, František a kolektiv. *Bezpečnost pro firmu, úřad, občana*, Praha, Public History, 2001, ISBN 80-86445-04-6.

kvalitní profesní úrovně organizace poskytující bezpečnostní služby, zejména v oblasti bezpečnostního poradenství.

V oblasti **politiky** nás bude zajímat především, zda v důsledku mezinárodních smluv a dohod nedojde ke změnám vnitřních předpisů a norem, upravujících oblast bezpečnosti organizace. Jedná se například o vstup České republiky do Evropské unie pro oblast zabezpečení, z toho vyplývající nové technické normy, které se dotknou zabezpečovacích technologií, nové předpisy z oblasti bezpečnosti práce, závazné použití určitých bezpečnostních standardů při provozu počítačových sítí atd. Pracovníky bezpečnostního průmyslu též může zajímat aktualizace požadavku na zabezpečení organizace při uzavírání pojistek a jejich podmínky obecně.

Obor **ekonomiky** je pro práci s naší analýzou také velmi důležitý, protože organizace jsou subjekty ekonomiky působící na hospodářském trhu a mírou jejich úspěšnosti je dosažená úroveň ekonomických výsledků. Vše, co může ovlivnit výsledek hospodaření společnosti, může mít v důsledku vliv na systém zabezpečení organizace. V ekonomické oblasti nás zajímají také události a trendy, které nemusejí bezprostředně ovlivnit hospodářské postavení organizace samotné, ale mohou se dotknout problematiky zabezpečení organizace přímo. Zvýšení cen určitých komodit, nebo služeb z oblasti bezpečnostního průmyslu bude mít přímý vliv na ekonomiku provozu bezpečnostního systému organizace.

**Sociální** oblast je charakterizována dominantním lidským prvkem, z toho důvodu události a trendy mohou mít zásadní vliv na organizaci jako celek i na jednotlivé oblasti její činnosti včetně zabezpečení. Negativní pohyby v oblasti sociální jsou provázeny i negativními pohyby v oblasti obecné kriminality, jde o skutečnost, které musíme věnovat pozornost. Nemusí však být pravidlem, že nepříznivý vývoj v sociální oblasti vždy působí v organizaci negativním přínosem pro její zabezpečení. Fakt vzrůstu nezaměstnanosti nás může vést k úvahám o větší kriminalitě a následně zvýšené hrozbě odcizení majetku organizace, a tedy k důkladnější potřebě fyzického zabezpečení ostrahy objektu. Podle této úvahy bychom mohli využít například nezaměstnanosti středoškoláků a vysokoškoláků v rámci personálního zajištění bezpečnosti organizace a tím zvýšit její kvalitu zabezpečení. V rámci zlepšení sociálních a pracovních podmínek může zákonodárce stanovit maximální počet možných přesčasových hodin. Je velmi pravděpodobné, že z hlediska nasazení fyzické ostrahy bude nutné zvážit stávající rozdělení služeb strážných, a není vyloučeno, že organizaci donutí k náboru nových pracovníků ostrahy, či změně podmínek s bezpečnostní

agenturou, která nám tyto služby dodává. Takové změny právních předpisů mohou být na první pohled méně významné, avšak v důsledku mohou zasáhnout organizace velmi silně.

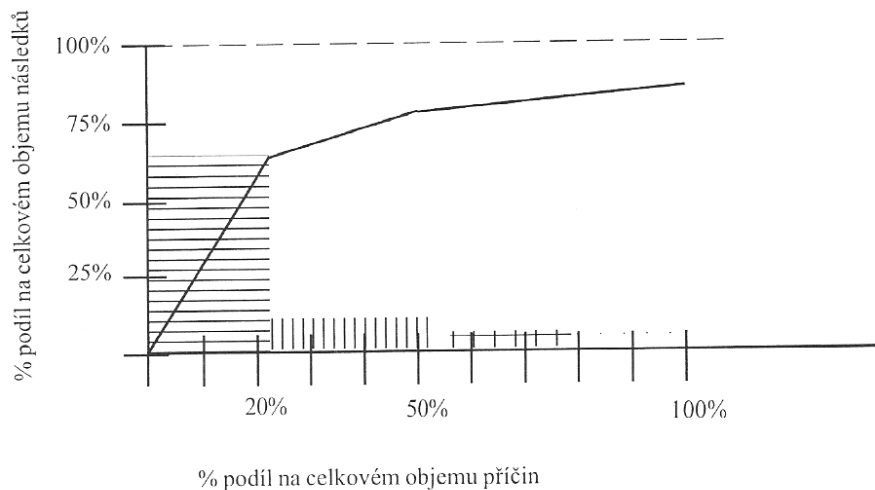
V oblasti **technologie** dochází k událostem a trendům, které mohou ovlivnit bezpečnostní systém velmi zásadním způsobem. Jedná se o vznik nových technologií v oblasti bezpečnostního průmyslu. V problematice výpočetní techniky má zásadní vliv vývoj nového hardwaru a softwaru na bezpečnost provozu počítačových sítí, ale i pro získávání a analýzu potřebných informací z různých oborů. Sebelepší a dokonalejší technika zastarává jak morálně, tak i fyzicky. Organizace, které dobře fungují, musí řešit otázku výměny staré techniky za novou technologii. Jedná se o požadavky na bezpečnost informací, které ke svému správnému fungování potřebují nejnovější produkty a aktualizace HW a SW. Velmi důležité je pochopit směr, kam se technologie ubírají a umět se učit, jaké požadavky na bezpečnost bude budoucnost vyžadovat. Pokud se tímto směrem organizace nevydá, může čekat, že přijme nesprávná řešení, nebo řešení ekonomicky neefektivní.

Hlavní a nespornou výhodou analýzy PEST je umožnění přípravy organizace na budoucí události a změny včas. Tím může eliminovat negativní dopady budoucích hrozeb. [17]

### 3.3 Paretova analýza

Jedná se o nejznámější kvantitativní techniku, kterou vedení firmy běžně při analyzování příčin, jež stojí za důsledky, používá. Jedná se o nepříliš komplikovanou, ale také nepřiliš přesnou techniku. Její duchovní otec je Wilfred Pareto, ekonom 19. století, který při zkoumání populace v Itálii postřehl, že 80 % majetku je vlastněno pouze 20 % obyvatelstva. Tato technika se také může nazývat pravidlem 80/20. Bylo zjištěno, že toto pravidlo najde aplikaci v mnoha oblastech života. V oblasti ekonomiky můžeme toho pravidlo vyjádřit slovy: 20% úsilí produkuje 80% efektu – v analýze příčin pak platí, že za 80 % následků stojí 20 % příčin. Díky své jednoduchosti, s kterou lze aplikovat na zkoumaný problém, nachází tato metoda uplatnění při zpracování bezpečnostní analýzy. Zaměřuje se na vztah mezi příčinou, následkem a schopností vyjádřit tyto vztahy v kvantifikované podobě. K jejímu sestrojení je nutné kvantifikovat a seřadit sebrané údaje v sestupném pořadí podle určitých kritérií, která si stanovíme. Například se může jednat o četnost výskytu, nebo o velikost rozsahu následné škody atd. Na svislou osu vyneseme např. kumulativní relativní

četnost<sup>9</sup> příčin v procentech a na vodorovnou osu jejich kumulativní podíl na celkovém množství důsledků také v procentech.



Obr. 5 Parettův diagram<sup>10</sup>

Tato analýza není metodou, která by nám pomohla vyřešit vše – dá se použít téměř na každý problém, nedá se však použít na všechny problémy současně. Jednotlivé problémy je třeba analyzovat odděleně.

Hlavní přínos této techniky je v tom, že nám ukáže, kam zaměřit svou pozornost. Další vylepšení při tvorbě analýzy může být použití modifikované analýzy stupně ohrožení, včetně znázornění v krizové matici - tato metoda se používá v oblasti krizového managementu. Analýza stupně ohrožení si dává za cíl zjistit, jaká je pravděpodobnost, že nastane určitá krize či konflikt a jaké budou její účinky (následky), když skutečně nastane. Zde je velmi důležité přesné určení pracovních kroků, v první fázi je třeba možné krize či konflikty pojmenovat. V druhé fázi je nutné vymezit posuzované období, protože s přibývajícím délkou posuzovaného období se zvyšuje pravděpodobnost, že krize nastane. Nejtěžší třetí fáze je stanovení stupně pravděpodobnosti. Zde použijeme zpravidla subjektivní hodnocení

<sup>9</sup> Postupně načítaná četnost jednotlivých (vzestupně uspořádaných) hodnot znaku ve statistickém souboru

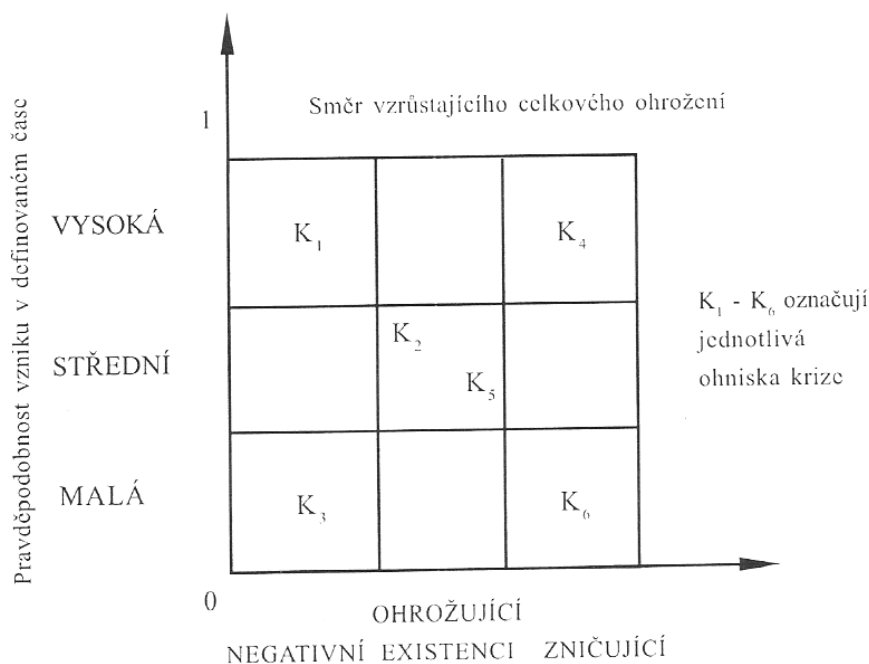
<sup>10</sup> Převzato z: BRABEC, František a kolektiv. *Bezpečnost pro firmu, úřad, občana*, Praha, Public History, 2001, ISBN 80-86445-04-6.

založeného na naší zkušenosti. Maximální pravděpodobnost je vyjádřena hodnotou 1,0 – tj. jistota, že krize nastane v předpověděném období. Ve čtvrté fázi se stanoví účinky krize, protože právě účinky mohou zasáhnout mnoho oblastí činnosti organizace. Zde se hlavně budeme zajímat o oblast zabezpečení organizace.

Během práce s touto metodou používáme připravené formuláře, které pomáhají graficky a písemně znázornit dílčí poznatky, jako je například schéma pro stanovení posuzovaného období, schéma stanovení polohy ohnisek krize v matici. V poslední páté fázi je nutné zapsat hodnocení do připraveného formuláře a konečné přenesení do matice. [3]

### 3.3.1 Krizová matice

Tato matice představuje graficky ohraničenou plochu v podobě obdélníku rozděleného podélně a svisle na celkových devět polí.



Obr. 6 Krizová matice podle Klause Winterlinga <sup>11</sup>

Po umístění jednotlivých ohnisek krize do krizové matice musíme provést také jejich hodnocení. Matice přehledně zobrazuje celkové ohrožení organizace a dle umístění jednotlivých krizí v matici můžeme posuzovat, jak závažné krize hrozí organizaci a jaká bude vol-

<sup>11</sup> Převzato z: BRABEC, František a kolektiv. *Bezpečnost pro firmu, úřad, občana*, Praha, Public History, 2001, ISBN 80-86445-04-6.

ba strategie pro úspěšné vyvedení organizace z krizové situace. Čím větší četnost ohnisek krize v pravém horním obdélníku, tím větší problémy bude muset organizace řešit. Je však špatné spokojit se s pocitem, že krize takto vyjádřené mohou nastat jen velmi nepravděpodobně. Z praxe je známý princip kumulace počtu pravděpodobností, které jsou na sobě nezávislé. Tato metoda je vhodná jak pro zpracování komplexní bezpečnostní analýzy organizace, tak pro zpracování dílčí bezpečnostní analýzy dílčího bezpečnostního problému. Tato metoda nám umožní zpracovat analýzu účinků jednotlivých krizí jak na celou organizaci, tak jen na systém zabezpečení organizace či jeho části. Mluvíme například o technickém zabezpečení či zabezpečení informačního systému apod. Krizi je nutné definovat a popsat – je tedy třeba spolupráce analytiků s vybraným personálem organizace. Práce na řešení krizových situací, se kterými se může organizace setkat při své činnosti, je nezbytným předpokladem pro bezkonfliktní rozvoj organizace i v budoucnu. Můžeme se také setkat s případy, kdy krizové plánování a příprava na řešení budoucích krizí, či mimořádných situací je povinností, kterou organizaci ukládá přímo zákon. Jednalo by se zde o povinnost zpracovat krizový plán ochrany objektu podle vyhlášky NBÚ č. 339/1999 Sb. O objektové bezpečnosti.<sup>12</sup> [3] [21]

### 3.4 Analýza stromem poruch FTA

Jedná se o deduktivní metodu vyhledávající jednotlivé havárie, nebo systémové poruchy a určuje příčiny těchto událostí. FTA je grafický model různých kombinací poruch zařízení a lidských chyb, které by mohly vyústit v hlavní systémovou poruchu nazývanou „vrcholová událost“.

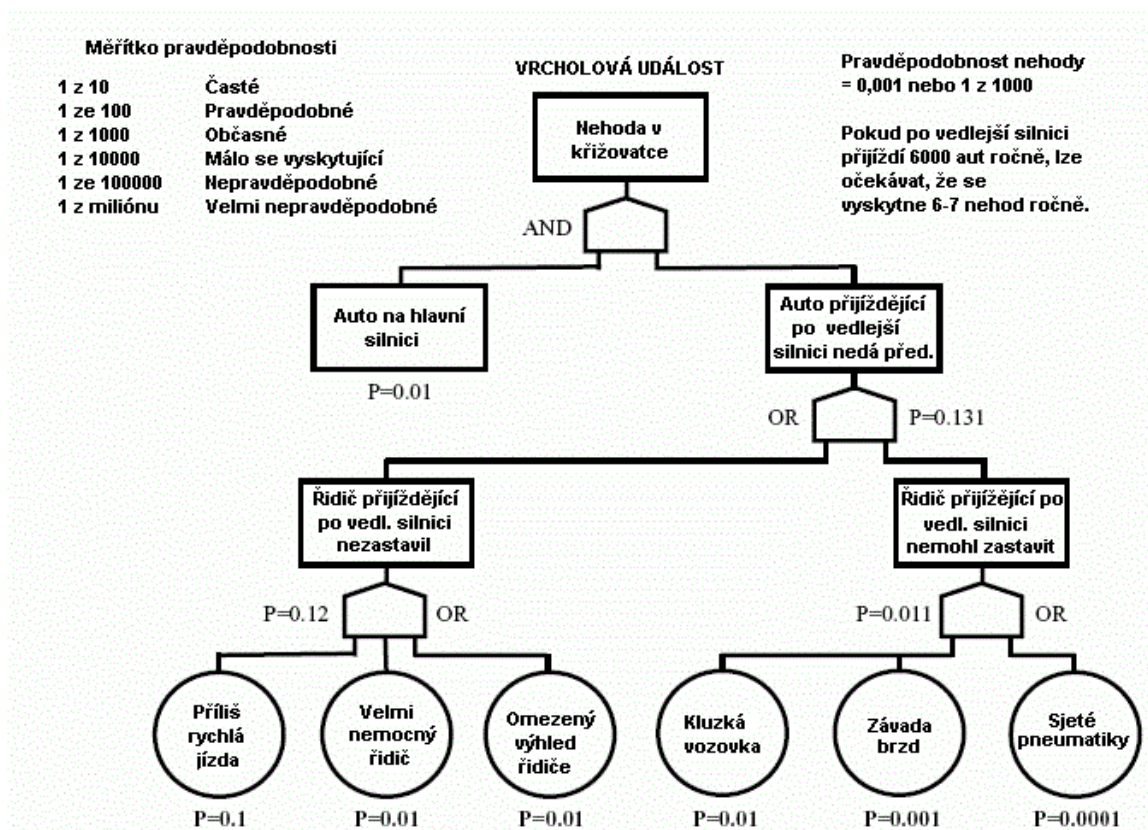
Metoda je vhodná i pro rozsáhlé systémy, může stanovit úplný výčet minimálních poruch. Model je založen na Booleovské algebře (hradla „a“, „nebo“ a jiné) při vyhledávání minimální poruchy vedoucí k vrcholové události.

---

<sup>12</sup> Tato vyhláška stanoví způsob zabezpečení ochrany objektů, technické prostředky, použití technických prostředků, podmínky nasazení fyzické ostrahy a režimová opatření pro účely objektové bezpečnosti.

Výsledkem budou typy poruch a kvantitativně přiřazené pravděpodobnosti poruch systémů, pokud známe pravděpodobnosti primárních příčin. Tato metoda umožňuje analytikovi zaměřit se na preventivní nebo zmírňující opatření týkající se významných základních příčin tak, aby byla snížena pravděpodobnost vzniku nehody.

Analýzu může provádět jeden, nebo více analytiků, kteří mohou doporučit bezpečnostní zlepšení procesu. Metoda se nehodí pro rané fáze projektování, je náročná na čas a náročnost se zvyšuje v závislosti na složitosti systému. [5]



Obr. 7 Analýza FTA <sup>13</sup>

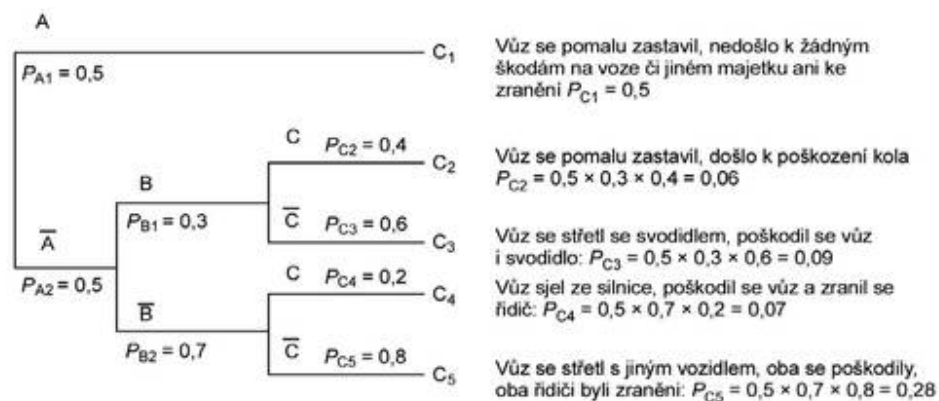
### 3.5 Analýza stromem událostí ETA

Metoda ukazuje možné koncové stavy nějaké nehody, která následovala po iniciační události<sup>14</sup>. Analýza stromu událostí uvažuje odezvy bezpečnostních systémů a operátorů na

<sup>13</sup> Převzato z: Metoda analýzy FTA. *Ikvalita.cz: Portál pro kvalitaře* [online]. [cit. 2014-05-01]. Dostupné z: <http://www.ikvalita.cz/tools.php?ID=52>

<sup>14</sup> Určitá porucha zařízení, nebo lidská chyba.

iniciační události a určuje možné koncové stavy této nehody. Výsledkem analýzy ETA jsou scénáře nehody, tedy soubor poruch nebo chyb, které vedou k nehodě. Tyto výsledky popisují možné koncové stavy nehody pomocí sekvence událostí<sup>15</sup>, které následují po iniciační události. Tato metoda je vhodná pro analýzu složitých procesů, které mají několik úrovní bezpečnostních systémů nebo postupů pro případ nouze, vhodných pro odezvu na určité iniciační události. Stromy událostí jsou využívány pro identifikaci různých nehod, které se mohou objevit u složitého procesu. Po identifikaci těchto nehodových sekvencí mohou být určeny typické kombinace poruch pomocí analýzy stromu poruch, které mohou vést k těmto nehodám. Rozdíl mezi analýzou stromem poruch a stromem událostí je, že FTA postupuje od vrcholové události k jejím příčinám a vyhledává základní události, kterým je možné přiřadit pravděpodobnost. Naproti tomu ETA se nezabývá příčinami nežádoucí události, ale zvažuje její další rozvoj, a tak poskytuje přehled o výši pravděpodobností možných výsledných událostí. Výsledkem jsou tedy modely stromu událostí a úspěchy nebo neúspěchy bezpečnostních systémů, které vedou ke každému definovanému koncovému stavu. Analýza může být provedena jedním analytikem, ale 2 – 4 jsou často preferováni. Analytici používají těchto výsledků pro identifikaci projektových a procesních slabých míst a poskytují doporučení pro snížení pravděpodobnosti nebo následků analyzovaných možných nehod. [5] [15]

Obr. 8 Analýza ETA<sup>16</sup>

<sup>15</sup> Úspěchy nebo selhání bezpečnostních funkcí

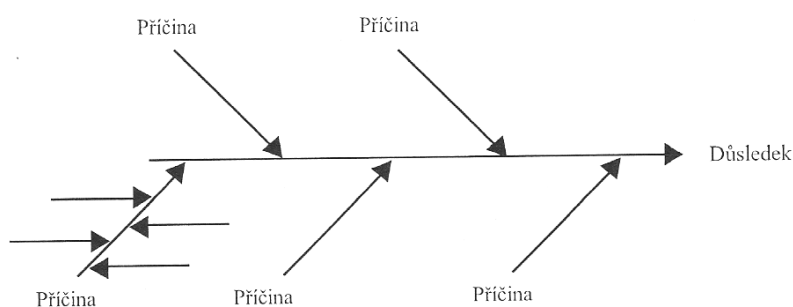
<sup>16</sup> Převzato z: *QM Profí: Analýza stromu událostí* [online]. 2014 [cit. 2014-05-21]. Dostupné z: <http://www.qmprofi.cz/33/analiza-stromu-udalosti-eta>

### 3.6 Analýza příčin a následků CCA

Tato analýza je směsí analýzy stromem poruch a Analýzy stromem událostí. Výhoda metody spočívá ve využití jako komunikačního nástroje: diagram zobrazuje vztahy mezi havarijními následky a jejich základními příčinami. CCA je metoda použitelná v jednoduchých případech poruch, zahrnuje výsledky obou analýz do stejného diagramu. Výsledkem analýzy je popis potenciálních havarijních výsledků, v diagramu lze sledovat havarijní sekvence – scénáře havárií. Pro tuto metodu je výhodnější malý tým o dvou až čtyřech osobách s různými zkušenostmi, jeden z nich se znalostmi metody CCA. Na tuto metodu navazuje a úzce s ní souvisí další způsob analýzy a to Išikavův diagram. [15]

### 3.7 Išikavův diagram

Hovoříme o praktickém pomocníku při zpracování bezpečnostní analýzy, též známém pod názvem diagram příčin a důsledků nebo pod názvem rybí kost. Diagram nám pomůže velmi jednoduše znázornit konkrétní analyzovaný problém z hlediska jeho příčin. Tato jednoduše spočívá pouze v jeho grafickém znázornění, nikoliv v jeho správném sestavení. Svým vzhledem připomíná větvení rybí kosti, jak již jeden z názvů napovídá. Přesný formát diagramu závisí především na specifikách konkrétního řešeného problému. Tím určíme počet hlavních i vedlejších větví. Išikavův diagram znázorňuje všechny příčiny, které se k danému problému vztahují. [3]



Obr. 9 Išikavův diagram <sup>17</sup>

<sup>17</sup> Převzato z: BRABEC, František a kolektiv. *Bezpečnost pro firmu, úřad, občana*, Praha, Public History, 2001, ISBN 80-86445-04-6.

Odborná literatura popisuje základní kategorie příčin, jde v zásadě o pět hlavních kategorií: lidská pracovní síla, stroje, metody, materiály, měření (nebo informace). Tyto kategorie jsou důležité především pro výrobní organizace ve vztahu k problémům spojených s jakostí výrobků. V oblasti služeb je struktura problémů proměnlivější. Ta však úzce souvisí s problémem, který má být analyzován. Pokud se zabýváme komplexní bezpečností organizace, je nezbytné určit kategorie příčin, které skutečně s problémem souvisí. Mluvíme tedy o těchto základních kategoriích příčin: zaměstnanci, ostatní fyzické osoby, bezpečnostní technika, dodavatelé služeb a technologií pro oblast bezpečnosti, metody, informace (tj. informační technologie a informační systémy), systémy a vnější prostředí.

### 3.7.1 Rozdělení do kategorií

Tyto základní kategorie také budou sloužit jako hlavní větve našeho diagramu. V jednotlivých kategoriích příčin je zapotřebí příčiny konkretizovat, tj. z hlediska diagramu vytyčit i vedlejší větve. Ty můžeme tvořit například takto:

1. Kategorie zaměstnanci
  - Systém výběru zaměstnanců (funkce, které mají význam z hlediska bezpečnosti organizace)
  - Úroveň kvalifikace zaměstnanců (ti, kteří se podílí na systému bezpečnosti organizace)
  - Kvalita a úroveň komunikace mezi zaměstnanci, řízení zaměstnanců, sociální program a tvorba motivace (zejména u zaměstnanců na bezpečnostně citlivých místech v organizaci)
2. Kategorie zabezpečovací technika
  - Funkčnost
  - Morální a fyzická opotřebovanost
  - Kvalifikovanost obsluhy
  - Úroveň servisu
3. Kategorie ostatní fyzické osoby
  - Kontrola pohybu cizích osob po areálu organizace
4. Kategorie dodavatelé technologií a služeb souvisejících s bezpečností organizace

- Počet dodavatelů
- Bezpečnostní úroveň dodavatelských organizací
- Ekonomická stabilita dodavatelských organizací
- Míra závislosti na dodavatelích bezpečnostních služeb a technologií
- Bezpečnostní prověrka zaměstnanců dodavatele

#### 5. Kategorie metody

- Úroveň kontrolních mechanismů v oblasti bezpečnosti
- Existence zpětné vazby
- Existence a kvalita signalizace hrozeb
- Řídící úroveň vedoucích pracovníků

#### 6. Kategorie informace

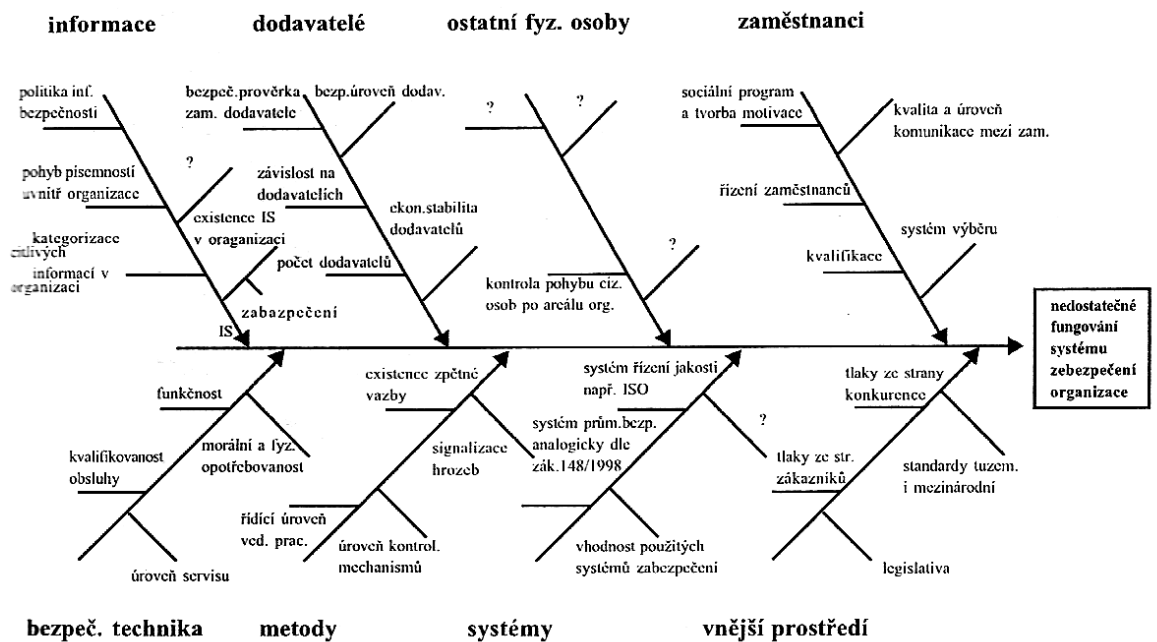
- Existence informačního systému v organizaci
- Úroveň bezpečnostní ochrany informačního systému organizace
- Existence institutu citlivých informací uvnitř organizace
- Existence politiky informační bezpečnosti
- Pohyb písemností uvnitř organizace, tj. administrativní bezpečnost

#### 7. Kategorie systémy

- Vhodnost použitých systému zabezpečení
- Existence systému řízení jakosti v organizaci, např. ISO
- Systém průmyslové bezpečnosti podle zákona č. 148/1998 Sb., případně analogický systém – systém objektový [20]

#### 8. Kategorie vnější prostředí

- Legislativa
- Standardy tuzemské i mezinárodní
- Požadavky a tlaky ze strany zákazníků
- Tlaky ze strany konkurence



Obr. 10 Znáornění příčin nedostatečného fungování bezpečnostního systému organizace<sup>18</sup>

### 3.7.2 Výhody diagramu

Mezi výhody Išikavova diagramu patří možnost použití nejen pro hledání příčin určitých následků, k nimž může patřit například nedostatečné zabezpečení organizace, ale také pro hledání řešení, jak dosáhnout žádoucího stavu (hledání alternativ). V tomto případě však diagram zobrazujeme otočený tak, že požadovaný stav si napíšeme vlevo a od něj vpravo vytyčíme hlavní a vedlejší větve, ve kterých uvedeme oblasti, kde budeme hledat řešení. Zpravidla jsou tyto oblasti totožné s těmi, které jsme definovali již při analýze příčin. [3]

<sup>18</sup> Převzato z: BRABEC, František a kolektiv. *Bezpečnost pro firmu, úřad, občana*, Praha, Public History, 2001, ISBN 80-86445-04-6.

## 4 BEZPEČNOSTNÍ PROGNÓZA

Jen určitá úroveň poznání nám umožňuje hledat a nalézt relevantní otázky a odpovědi, které jsme v rámci formulovaného problému položili. Mezi metody, pomocí kterých získáme potřebné znalosti o problému, který řešíme, patří analýza spojená se syntézou. Ta však sama o sobě není zcela dostačující, protože z ní získáme především poznatky o tom, jak se události a jevy udály v minulosti nebo jak se dějí i v současnosti a co je jejich příčinou. My však neřešíme problémy minulosti, ale budoucnosti.

### 4.1 Cíle bezpečnostní prognózy

Naším cílem je nalézt řešení, které ob stojí co nejdéle a odolá všem změnám prostředí. Poznáváme tedy i budoucnost, abychom poznání budoucího vývoje mohli zahrnout do svých znalostí minulosti a přítomnosti. Naše snaha o poznání problémů, musí být ucelená – komplexní. Prognózování nám umožní tento proces dosud známého poznání povýšit na vyšší úroveň. Budoucnost se vyznačuje vysokou mírou neurčitosti, pomocí prognózování jsme schopni tuto míru neurčitosti snížit. Platí pravidlo, že pokud bude naše prognózování přesnější, tím bude pro nás plánování jednodušší. Základní myšlenkou prognózování je soustředění se na předvídaní budoucího vývoje prostředí a na vznik podmínek, které nastanou v budoucnu a které budou mít vliv na problém, který řešíme v současnosti. Prognózování tvoří základ pro bezpečnostní plánování a posuzuje námi navržená alternativní řešení v kontextu s budoucími podmínkami. S výsledky prognózy je spjata řada trendů mezinárodních, politických, makroekonomických či konkurenčních atp. [3]

### 4.2 Použití bezpečnostní prognózy

Proces prognózy je běžnou součástí plánovacího procesu ve většině organizací, proto se jedná o metodu obvyklou. Organizace jej využívá především jako celek, ale je možné jej také použít na řešení dílčích problémů v jednotlivých činnostech organizace. Samozřejmě, že v oblasti bezpečnosti organizace má prognózování své nezaměnitelné místo. Bezpečnostní prognózování se vyznačuje určitými nuancemi oproti jiným druhům prognózování, které se v organizaci standardně provádějí. Jde především o oblast jeho zaměření – je to poznávací proces, zabývající se jevy a událostmi, které mají přímou nebo nepřímou vazbu na bezpečnost organizace a které udávají nebo výrazně ovlivňují směr nutného dalšího bezpečnostního vývoje společnosti ve sledovaném čase. Bezpečnost organizace a její bezpečnostní strategie tvoří jen subsystém v rámci systému celkové strategie organizace, bude

tedy i bezpečnostní prognóza ovlivňována závěry prognóz z ostatních oblastí činnosti organizace. Jelikož se jedná o metodu, u které pracujeme s mírou pravděpodobnosti (přesněji tedy s mírou nejistoty) musí být její výsledek v průběhu sledovaného období postupně porovnáván se skutečným vývojem. Organizace tedy musí mít k dispozici účinný monitorovací systém – buď vlastní, nebo poskytnutý –, který jí umožní sledování skutečného průběhu realizace rozhodnutí. Pokud porovnáme realizaci plánovaného průběhu se skutečným, bývají zpravidla odhaleny významné odchylky. Měla by tedy následovat analýza příčin těchto odchylek a můžeme následně tyto informace použít ke korekci původní prognózy.

#### **4.2.1 Kvantitativní a kvalitativní přístup**

Mezi další významné odlišnosti od jiných typů prognóz patří skutečnost, že v oblasti zabezpečení organizace pracujeme zpravidla s informacemi, jevy a událostmi, které můžeme jen částečně kvantifikovat. Tato skutečnost významně ovlivní výběr prognostických technik, které při zpracování prognózy můžeme použít. Nepomůže nám tedy ani základní členění prognostických metod na kvalitativní a kvantitativní, protože některé kvalitativní metody vycházejí a produkují číselné výsledky a v opačném případě některé kvantitativní metody používají subjektivní hlediska hodnocení. V rámci bezpečnostní problematiky při zpracování jednotlivých dílčích bezpečnostních prognóz, dotýkajících se jen dílčí problematiky, můžeme využít metod kvantitativních. Může se jednat například o úroveň zabezpečení formou bezpečnostní techniky. Pro celek však obecně platí, že naše závěry se budou často opírat o metody kvalitativní – odhadové. [3]

### **4.3 Rozdělení metod**

Ke kvalitativním metodám patří zejména osobní hodnocení, panelová shoda a metoda Delphi. Mezi kvantitativní metody, které u bezpečnostní prognózy můžeme použít, patří především projektování trendů, a to metoda klouzavých průměrů, exponenciální vyrovnávání a modely časových řad.

#### **4.3.1 Osobní hodnocení**

V praxi zřejmě nejčastěji užívaná metoda, jejíž podstata spočívá v tom, že jednotlivec – nejčastěji vedoucí pracovník organizace – subjektivně předvídá budoucnost. Spolehlivost a přesnost této metody je velice sporná, v mnohém záleží na odbornosti a zkušenosti jednotlivce, provádějícího předpověď. Metodu lze aplikovat i tam, kde nejsou k dispozici žádná

statistická data, nebo tam, kde nám tato data nemohou dát dostatečnou odpověď. Tato metoda je použitelná zejména pro krátkodobé předpovědi provozního charakteru.

#### 4.3.2 Panelová shoda

Tato technika na rozdíl od předchozí metody částečně omezuje vliv osobních postojů a myšlenkových stereotypů prognózujícího jedince tím, že předpovídajícím subjektem není jednotlivec, ale kolektiv. Jde o kolektiv osob na určité odborné úrovni, mající znalost bezpečnostní problematiky a zejména znalost v oblasti komerční bezpečnosti. Vzájemným sdílením svých postojů a názorů se účastníci snaží dojít ke společné shodě, která reprezentuje předpokládaný vývoj. Při realizaci této metody je velmi důležité, jakým způsobem je dosaženo společné shody a jak je celý proces skupinového myšlení usměrňován.

#### 4.3.3 Metoda Delphi

Tato metoda je podobná metodě předchozí, stejně jako panelová shoda využívá úsudku kolektivu odborníků. Avšak jiným způsobem pracovníci týmu neprovádějí prognózování společně, nýbrž odděleně. Dokonce ani nevědí, kdo patří mezi další členy týmu. Každý odborník vyplňuje své hodnocení samostatně do předem připraveného dotazníku. Poté jsou dotazníky od odborníků vybrány, sumarizovány a vráceny zpět expertům. Každý z nich má možnost své stanovisko přehodnotit a zrevidovat s ohledem na názor ostatních členů týmu. Takto postupují tak dlouho, dokud není dosaženo společné shody, nebo případně dokud se nenaplní počet předem domluvených kol hodnocení. Nevýhodou této metody je časová a organizační náročnost, mezi výhody patří zejména anonymita účastníků.

#### 4.3.4 Metoda klouzavých průměrů

Řadí se již mezi kvantitativní prognostické metody a lze ji s úspěchem použít i v oblasti bezpečnostního prognózování. Pro představu si uveďme, že bychom rádi zjistili, jaký je dosavadní vývoj určité veličiny důležité pro posouzení úrovně bezpečnosti organizace, a na základě dosavadního vývoje předpověděli její vývoj budoucí – k tomu je zejména tato metoda určena. Pro příklad můžeme uvedenou metodu použít při prognóze počtu krádeží zboží v obchodním domě. Výsledkem bude grafické znázornění, například v podobě lineárního spojnicového grafu, kde na svislou osu vyneseme údaje o počtu krádeží a na osu vodorovnou vyneseme časové celky (dny, týdny, čtvrtletí), kdy ke krádežím docházelo. Pokud budeme sledovat krátké období, například několik málo týdnů, pak bude naše prognóza v podstatě aritmetickým průměrem hodnot z předchozích týdnů. Pokud však pro

předpověď vývoje použijeme velký počet předchozích týdnů, nebudeme schopni vzít v úvahu například výrazné změny, ke kterým došlo v nejbližších předchozích týdnech. Proto tedy nepoužijeme běžný aritmetický průměr ze všech předchozích období, ale takzvaný průměr klouzavý – průměr z předem stanoveného počtu posledních týdnů. Tento způsob předpovědi je použitelný zejména pro krátkodobé předpovědi.

#### 4.3.5 Metoda exponenciálního vyrovnání

Upřesňuje metodu klouzavých průměrů tím, že odlišuje význam jednotlivých údajů dle toho, zda se jedná o údaje staršího či novějšího data. Metoda klouzavých průměrů si klade dvě zásadní otázky: kolik má být při aplikaci této metody použito časových intervalů a zda je správné, aby jednotlivé skutečné údaje měly pro určování prognózy vždy stejný význam. Pro přesnější prognózy mají zpravidla větší význam metody data novějšího než data staršího. Metodu, která stanoví vyšší hodnotu pro údaje aktuální a nižší pro údaje starší, nazýváme metodou exponenciálního vyrovnání. V praxi jde o výpočet váženého klouzavého průměru skutečných hodnot, kde aktuálnější mají větší váhu, než ty ostatní. Pro management tato metoda působí určitý problém, jak by měly být velké jednotlivé váhy.

#### 4.3.6 Prognostické modely

Respektují určité trendy nebo sezónní výkyvy, tudíž jsou důležitou oblastí. Tyto modely časových řad pracují se třemi základními složkami: trendovou, sezónní a náhodnou. Trend představuje rozhodující tendenci dlouhodobého vývoje analyzované proměnné veličiny. V tento moment není rozhodující, zda je stoupající, či klesající, nebo zda má stabilní průběh. Ukazuje, jak se sledovaná veličina bude dlouhodobě vyvíjet. Sezónní složka nám znázorní pravidelné kolísání sledovaného ukazatele okolo trendu v průběhu sledovaného období. Pro sezónní složku je charakteristické, že se v souměřitelných časových obdobích (každý rok) pravidelně opakuje. Například počet krádeží v obchodním centru vykazuje pravidelně nárůst v období před Vánoci, kolem Velikonoc atd. Náhodná složka trendu znázorňuje nepředvídatelné rozkolísání skutečných hodnot kolem hodnot předpokládaných. Tyto výkyvy mohou být způsobeny i drobnými příčinami, které se v praxi těžko odhadují. Z toho vyplývá, že nepředvídatelné příčiny náhodné složky trendu nelze předem stanovit, a proto na vlastní stanovení předpovědi (prognózy) nemají vliv. K náhodným vlivům v případě vývoje počtu krádeží v obchodním centru může například patřit nepředvídané uzavření některých prodejních oddělení z důvodu rekonstrukce. Cílem analýzy časových řad je vyjádření jejich trendové a sezónní složky v kvantifikované podobě. Proces kvantifi-

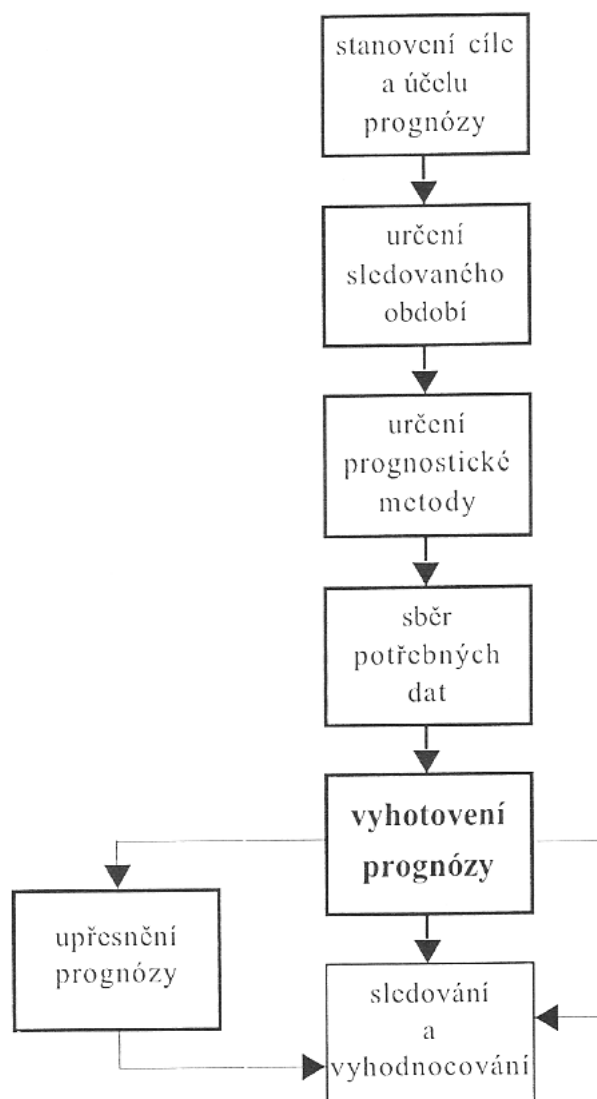
kace těchto složek nazýváme dekompozicí časových řad. Tímto postupem jsme schopni příkladně stanovit trend vývoje kapesních krádeží v obchodním centru s předpokládanými sezónními výkyvy, což nám pomůže například při plánování počtu bezpečnostních pracovníků v jednotlivých obdobích nebo dle dosažených výsledků určit nasazení bezpečnostní techniky (kamery, CCTV).

Samotný prognostický proces můžeme rozdělit do několika kroků:

- Stanovení účelu (cíle), kterého má být prognózou dosaženo
- Stanovení délky prognózovaného období a četnosti opakování prognóz
- Vybrání vhodné prognostické metody, nebo souboru metod
- Provedení sběru dat potřebných ke zpracování prognózy
- Vyhotovení vlastní prognózy
- Sledování prognózy a vyhodnocování její přesnosti
- Zpětné zohlednění nových dat získaných vyhodnocením a upřesněním v původní prognóze a následné upřesnění prognózy

#### 4.4 Vyhodnocení prognózy

Mezi další možné kroky prognostického procesu patří i určení spolehlivosti a vhodnosti prognózy. Pokud se jedná o zpětné zhodnocení nově získaných dat, není nezbytné, pokud nebudeme chtít prognózu dále zpřesňovat. Vyhodnocování přesnosti a sledování prognózy však musí být neoddelitelnou součástí prognostického procesu, jinak nemá význam prognózu vůbec vyhotovovat. [3]

Obr. 11 Prognostický proces<sup>19</sup>

---

<sup>19</sup> Převzato z: BRABEC, František a kolektiv. *Bezpečnost pro firmu, úřad, občana*, Praha, Public History, 2001, ISBN 80-86445-04-6.

## 5 HODNOCENÍ RIZIK

### 5.1 Aktivum

Vše co má pro organizaci nějakou hodnotu, která může být zmenšena působením hrozby.

- Aktiva hmotná (finanční prostředky, cenné papíry, nemovitosti, zboží atd.)
- Aktiva nehmotná (informace, kvalita personálu, autorská práva atd.)

Aktivem může být i subjekt organizace, hrozba totiž může působit na celou jeho existenci. Působením hrozby se aktivum vyznačuje určitou zranitelností, která může být minimalizována zavedením adekvátních bezpečnostních opatření.

### 5.2 Zdroj hrozby

Jakýkoliv faktor ovlivňující cíle, procesy, nebo projekty organizace.

- Vnější činitele (legislativní, či politické prostředí)
- Vnitřní činitele (procesy, zaměstnanci, nemovitosti)

Činitele aktivující konkrétní hrozby a jejich vývoj nebo činnost či nečinnost jsou příčinami možných nežádoucích dopadů na aktiva organizace.

### 5.3 Hrozba (Nebezpečí)

Vlastnost, síla, událost, aktivita nebo osoba, působící buď přímo na aktivum, nebo na bezpečnostní opatření s cílem získat přístup k aktivu. Aby mohla hrozba působit, musí být nejdříve aktivována, k čemuž slouží zdroj hrozby. Základní charakteristikou hrozby je její úroveň. Je hodnocena podle třech základních faktorů.

- Nebezpečnost (schopnost hrozby způsobit škodu)
- Přístup (pravděpodobnost, že hrozba svým působením získá přístup k aktivu)
- Motivace (zájem iniciovat hrozbu vůči aktivu)

#### 5.3.1 Klasifikace hrozeb

- Vnější hrozby – jsou neovlivnitelné, můžeme tlumit pouze důsledky jejich působení
  - Politické hrozby

- Ekonomické hrozby
- Sociální hrozby
- Technologické hrozby
- Legislativní hrozby
- Ekologické hrozby
- Vnitřní hrozby – ovlivnitelné, jejich působení můžeme minimalizovat, či eliminovat
  - **Procesní (projektové hrozby)**
    - Hrozby související s nastavením procesu (např. neexistence, nebo složitost pravidel či interních normativních aktů pro provádění procesu, neexistující, nebo špatně vymezené cíle procesu, nevhodná návaznost procesů, neexistující, nebo špatně vymezené kompetence, neefektivnost, nebo nepřesnost pracovních postupů)
    - Hrozby související se vstupy do procesu (např. včasnost dodání vstupů a kvalita vstupů)
    - Hrozby související se zdroji procesu (např. nedostatek zdrojů, nízká, nebo nevhodná kvalita zdrojů, špatná alokace zdrojů)
    - Hrozby související s výstupy procesu (např. včasnost dodání výstupů, kvalita výstupů)
  - Personální hrozby
  - Věcné hrozby (hrozby chemického, či fyzikálního charakteru)

## 5.4 Riziko

Vzniká vzájemným působením hrozby a aktiva. Vyjadřováno je kombinací resp. součinem pravděpodobnosti výskytu mimořádné události a jejího dopadu na dané aktivum. Je to tedy kvantifikace působení hrozby na aktivum. Riziko je možnost, že při zajišťování činnosti organizace s určitou pravděpodobností nastane určitá událost s následnými nežádoucími dopady na plnění schválených záměrů a cílů této organizace. Klasifikace rizik:

- Z hlediska předvídatelnosti (rizika předvídatelná a nepředvídatelná)

- Z hlediska ovlivnitelnosti (rizika ovlivnitelná a neovlivnitelná)
- Z hlediska původu (rizika primární a sekundární)
- Z hlediska objektivit hodnocení (rizika subjektivní a objektivní)
- Z hlediska dynamiky vývoje nežádoucí události (rizika pomalá a rychlá)
- Z hlediska pravděpodobnosti vzniku nežádoucí události (rizika pravděpodobná a nepravděpodobná)
- Z hlediska intenzity dopadu nežádoucí události (rizika s mírným, vyšším a fatálním dopadem)

## 5.5 Zranitelnost

Nedostatek, slabina nebo stav analyzovaného aktiva, které může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby. Zranitelnost vzniká tam, kde dochází k interakci mezi hrozbou a aktivem, základní charakteristikou zranitelnosti je její úroveň. Ta je stanovena dle dvou základních faktorů:

- Citlivosti (náchyllost aktiva být poškozeno danou hrozbou)
- Kritičnosti (významnost aktiva pro analyzovanou organizaci)

## 5.6 Bezpečnostní opatření

Proces nebo prostředek navržený za účelem minimalizace působení rizika, čehož může být dosaženo:

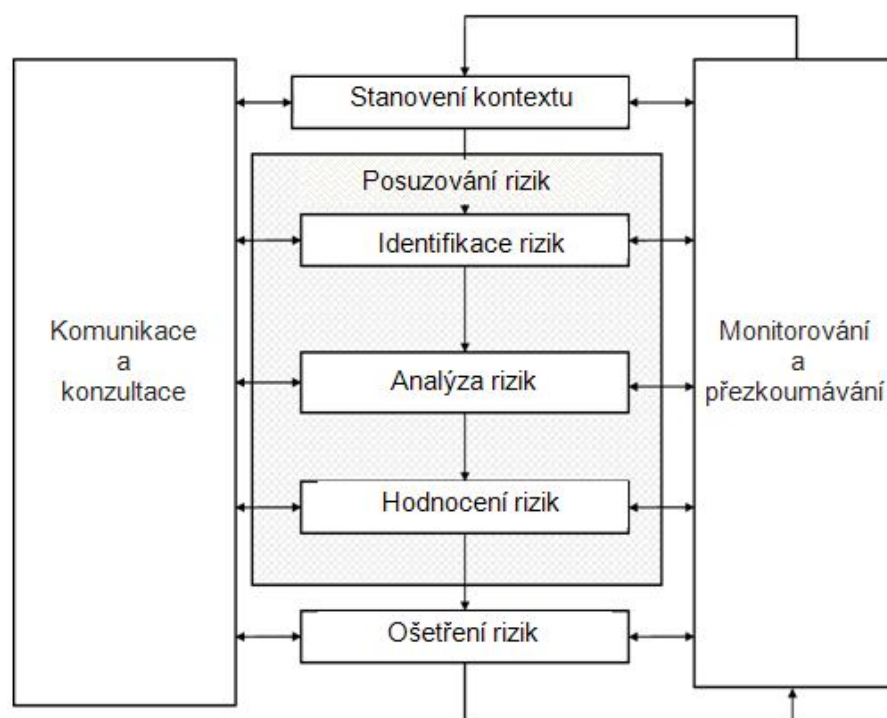
- Snížením zranitelnosti aktiva
- Eliminací zdrojů hrozeb
- Snížením pravděpodobnosti výskytu mimořádné události
- Snížením závažnosti dopadu mimořádné události

### Mimořádná událost

Nepříznivá a nežádoucí odchylka od očekávaného (žádoucího) výsledku nebo stavu, resp. závažná časově obtížně předvídatelná a prostorově ohraničená událost, způsobená vlivem antropogenní činnosti<sup>20</sup>, přírodních jevů či procesů, která ohrožuje život, zdraví, majetek nebo životní prostředí. V oblasti technologických rizik se pro tento pojem užívá termínu havárie. [11]

## 5.7 Řízení rizik

Jde o proces, při němž se organizace nebo subjekt snaží zamezit působení existujících nebo předpokládaných hrozeb a navrhuje řešení, která mají prostřednictvím vhodných bezpečnostních opatření minimalizovat závažnost dopadu, nebo pravděpodobnost výskytu mimořádných událostí. Pro úplnost upřesníme níže uvedené termíny: stanovení kontextu = vymezení souvislostí, ošetření rizik = zvládání rizik.



Obr. 12 Proces řízení rizik<sup>21</sup>

<sup>20</sup> Činností způsobené člověkem.

<sup>21</sup> Převzato z: ČSN ISO 31000. *Management rizik - Principy a směrnice*. 2010.

## 6 BEZPEČNOSTNÍ POLITIKA ORGANIZACE

Bezpečnostní politika organizace je souhrn odpovědí vrcholového vedení společnosti především na tři otázky:

- Co má organizace v oblasti bezpečnosti činit a z jakého důvodu
- Jakých cílů v oblasti bezpečnosti chce organizace dosáhnout
- Jak bude řídit jednotlivé podnikové činnosti a jaká budou následovat opatření, aby bylo dosaženo stanovených cílů

### 6.1 Podmínky bezpečnostní politiky

Pro efektivní fungování a účinné prosazení bezpečnostní politiky organizace je nezbytné, aby všechny zásady a opatření byly vyjádřeny v písemné formě. Dokument bezpečnostní politiky má charakter všeobecného plánu v oblasti bezpečnosti organizace a má velmi obecný charakter. Na základě posloupnosti celkových zájmů a cílů organizace vyplývá, že bezpečnostní politika musí být podřízena obecnému strategickému plánu organizace. Je to z toho důvodu, že bezpečnostní politika je jen jeden segment z celkové činnosti a není její rozhodující aktivitou. Prohlášení v dokumentu bezpečnostní politiky jsou obecná - zabírají celou šíři dané problematiky uvnitř organizace a jako takové nemohou být bez dalšího rozpracování použity k přímé realizaci. Rozhodujícím způsobem určují směr a způsob dalšího konání organizace v dané oblasti.

Bezpečnostní politiku ani obecnou politiku organizace nemůžeme zaměňovat s vizí organizace. Tato vize je spíše definice základního důvodu její existence a je vyjádřena zpravidla ve velmi obecné rovině. Základní kámen pro formulaci obecné bezpečnostní politiky je celková strategie organizace, proto tedy nelze vyloučit, že se bezpečnostní politika dostane do střetu se zájmy obecné politiky organizace. Například ekonomické cíle organizace a bezpečnostní cíle organizace nebývají zcela totožné a navzájem se nemusí vždy podporovat. Přesto by bezpečnostní cíle měly být otevřené a podřazené cílům ekonomickým. Současně s otázkami výše uvedenými by v dokumentu bezpečnostní politiky měla být zodpovězena další řada otázek:

- Kdo nese zodpovědnost za naplnění závěrů bezpečnostní politiky?
- Jaký je časový horizont pro naplnění cílů bezpečnostní politiky?
- Jak bude bezpečnostní politika uváděna do praxe?

- Jaké jsou na bezpečnostní politiku kladeny požadavky z hlediska efektivity nákladů?
- Jak bude dodržování zásad a cílů bezpečnostní politiky vynucováno, případně sankcionováno v případě porušení?

Pro upřesnění vztahu s bezpečnostním projektem je třeba uvést, že bezpečnostní projekt je konkretizací opatření a podrobným plánem realizace zásad a cílů stanovených bezpečnostní politikou. Bezpečnostní projekt je tedy na rozdíl od bezpečnostní politiky velmi konkrétní a podrobný, zaměřený na každý detail včetně sledování nákladů na realizaci.

## 6.2 Klasifikace

Problematika bezpečnosti organizace je velmi široká a zaměřuje se na tři základní oblasti: lidi, majetek a informace (zájmy). Problematiku uvedených třech oblastí bude řešit zároveň i obecná bezpečnostní politika organizace. Každou oblast, která je předmětem bezpečnostních zájmů organizace, formulujeme tak, jakoby se jednalo o samostatnou bezpečnostní politiku:

- Oblast personální
- Oblast organizační a administrativní
- Oblast ochrany majetku (objektová bezpečnost, politika ochrany majetku, politika ochrany nehmotného majetku)
- Oblast informačních systémů atd.

Přestože existuje vnitřní členění dokumentu bezpečnostní politiky dle výše uvedených kritérií, zůstávají formulace opatření a zásad v obecné rovině a jejich detailní rozpracování je ponecháno jednotlivým projektům. Jedním ze základních východisek při formulování základních bezpečnostních zásad bezpečnostní politiky organizace jsou tedy zásady obecné politiky organizace, které tvoří nepřekročitelný rámec pro formulaci zásad bezpečnostní politiky. Jak již bylo řečeno, v případě konfliktu mezi cílem bezpečnostní a obecné politiky by měly být upřednostněny cíle obecné politiky. Za určitých mimořádných okolností lze připustit, že cíle bezpečnostní politiky budou muset být naplněny i proti vůli organizace, včetně překročení rámce daného obecnou politikou a tudíž budou působit zpětně na formulaci zásad obecné politiky organizace. Obecné zásady tedy budou muset být korigovány, například v důsledku přijetí zákonů, které závazně stanoví v rámci bezpečnosti organizace

některá opatření, jejichž přijetí ovlivní původně formulovanou obecnou politiku organizace. Mezi další stanoviska zásad bezpečnostní politiky jsou vnější vlivy – okolnosti stojící mimo organizaci. Organizace tyto vlivy svým jednáním nemůže ovlivnit, případně jen částečně, může se jednat například o diskuzi o připravovaném zákoně apod. Jde o legislativní činnost státu, existenci různých závazkových vztahů ovlivňujících organizaci, konkurenční prostředí. Jsou to zejména mezinárodní smlouvy či smlouvy mezi podnikatelskými subjekty. Tyto vnější vlivy představují bariéry bezpečnostní politiky organizace. Dalším mezníkem pro stanovení zásad a cílů bezpečnostní politiky jsou vnitřní vlivy, tedy vnitřní bariéry pramenící z možností organizace samotné, které zpravidla může organizace svým jednáním ovlivnit. Hovoříme zde o ekonomických možnostech organizace, jejím organizačním uspořádání, úrovni řízení, úrovni personálního vybavení organizace, o technické úrovni, také o úrovni vnitřní komunikace atp. Jak vnější, tak vnitřní vlivy se podílely již na formulaci obecné politiky organizace. Přesněji jde o poznání těchto vlivů a pochopení jejich významu pro fungování organizace. V rámci formulace bezpečnostní politiky budou podrobeny opět analýze z hlediska jiných kritérií než při formulaci obecné politiky. Kritériem pro jejich zkoumání a pochopení jejich vlivu na bezpečnost organizace budou bezpečnostní hlediska. Zkoumáním vnějších a vnitřních okolností a jejich podrobení se cílenému procesu poznání (analýza, syntéza, prognóza) se opět dostáváme k hledání odpovědí na konkrétní otázky v rámci řešení specifických bezpečnostních problémů – úkolů organizace. Bezpečnostní politika představuje všeobecný plán organizace v oblasti bezpečnosti a tím tedy obsahuje konečný cíl a určitý termín. Nepřestává tedy existovat v okamžiku vytyčených cílů. Nejde o takový projekt, který by byl ukončen v okamžiku svého splnění. Cílem bezpečnostní politiky je dosažení určitého vztahu a úrovně bezpečnosti organizace. Zájmem organizace bude stav a úroveň, která bude trvat i do budoucna a bude trvalou součástí obecné strategie organizace. Bezpečnostní politiku je tedy možné chápat jako nepřetržitý proces, jehož obsahem je trvalé definování bezpečnostních zásad, opatření a potřeb organizace při naplňování celkové politiky organizace. Bezpečnostní politika představuje kompromis – často i bolestný mezi tím co organizace v bezpečnostní oblasti na jedné straně chce, může a smí a na druhé straně nechce, nemůže a nesmí. [3]

### 6.3 Přístupy k řešení otázky bezpečnostní politiky

Firemní bezpečnostní politiku se můžeme rozhodnout řešit dvěma způsoby. Forma, pro kterou se rozhodneme, bude záležet na několika parametrech, které níže budeme posuzovat.

#### 6.3.1 Krátká politika

Mezi kladné body vyplývající z krátké bezpečnostní politiky můžeme řadit:

- relativně snadná a rychlá příprava dokumentu
- jednodušší a rychlejší proces schvalování
- politika je poměrně neměnná a tudíž jí není třeba příliš často aktualizovat, bez problému se s politikou mohou seznámit všichni zaměstnanci

Na druhé straně mezi nevýhodami spatřujeme tyto skutečnosti: hlavní objem prací je přesunut do fáze rozpracování politiky do formy bezpečnostních standardů, vzhledem k rozsahu a obecnosti definovaných principů politika mnoho neřeší a v poslední řadě mezi zaměstnanci je problém si pod obecnými termíny představit jejich konkrétní naplňování.

#### 6.3.2 Rozsáhlá politika

Ke kladným stránkám rozsáhlé bezpečnostní politiky jednoznačně řadíme její velmi komplexní kodex upravující oblast informační bezpečnosti, kde se nacházejí definice hlavních principů a pravidel na jednom místě.

Vzhledem k detailům je eliminována případná desinterpretace či nepochopení, bezpečnostní standardy upravují velmi detailní a specifické oblasti bezpečnosti (informační bezpečnosti). Za záporné vlastnosti zmíníme časté změny, ke kterým v rámci bezpečnostní politiky dochází (při každé změně je třeba bezpečnostní politiku aktualizovat), práce na detailní politice mohou trvat neúměrně dlouho a existuje značné nebezpečí její nevyváženosti. Proces schvalování bývá dlouhý, komplikovaný s potřebou přijmout řady kompromisů. V poslední řadě se zmíníme o zaměstnancích, kteří se nemohou jednoduše seznámit s celou politikou a je potřeba pro jednotlivé organizační skupiny vytvořit speciální výtahy, které s sebou přinášejí další náklady. [7]

## 6.4 Problémy při tvorbě politiky

- Velké množství kompromisů – po procesu schvalování zbyla z původní verze jen část, problematické pasáže jsou vypuštěny nebo přepsány, pravomoci a zodpovědnosti jsou zredukovány na nezbytné minimum. Politika se stává sterilní a společnosti neumožní řešit to, co je skutečným problémem.
- Nereálná bezpečnostní politika – nesmírně přísná politika, společnost ji téměř v žádném bodě nevyhovuje. Nutná definice přechodného období a proces postupné implementace. Zaměstnanci seznámení s politikou celý proces vnímají odlišně od reality a budou ho jako celek ignorovat. Takový stav může vést k daleko horší situaci, než byla před zavedením politiky.
- Neadekvátní rozsah politiky – vedením je platnost působnosti odložena. Nemožnost seznámení managementu podrobně s celým dokumentem, nepochopení významu jednotlivých ustanovení. Strach z nereálných závazků a celkových negativních dopadů společnosti obvykle zpomalí, nebo dokonce zastaví proces schvalování bezpečnostní politiky.
- Podcenění propagace politiky – existence politiky často bývá před většinou zaměstnanců skryta. Je to podcenění, či nezvládnutí komunikace směrem dovnitř organizace. Sebelepší dokument nepomůže ničemu, pokud se s jeho obsahem neseznámí zaměstnanci a pokud se jím nebudou řídit.
- Nekritické přebírání vzorců – není zaručeno, že přenesení bezpečnostní politiky z jedné společnosti do druhé je zárukou kvalitní politiky. Vylepšování přejatých postupů bez předchozí analýzy může přinést velice špatný výsledek. [7]

## 6.5 Shrnutí bezpečnostní politiky jako prostředku bezpečnostního plánování

Zpracování bezpečnostní analýzy, bezpečnostní prognózy, zejména tedy bezpečnostního projektu (expertizy) je ovlivňováno bezpečnostní politikou organizace, která:

A) Vychází z

- Platných právních norem a jejich přímé aplikace či zprostředkované aplikace prostřednictvím firemních normativních aktů

- Specifik bezpečnostních požadavků na zajištění bezpečnostních zájmů organizace stanovených jejím vedením
- Představ vedení společnosti o požadovaném způsobu ochrany:
  - Vlastní podnikovou ochranou (hlídací službou atd.)
  - Dodavatelsky (soukromou bezpečnostní agenturou)
  - Popřípadě dle návrhu expertízy
- Ekonomických možností a ochoty financování ochrany bezpečnosti organizace

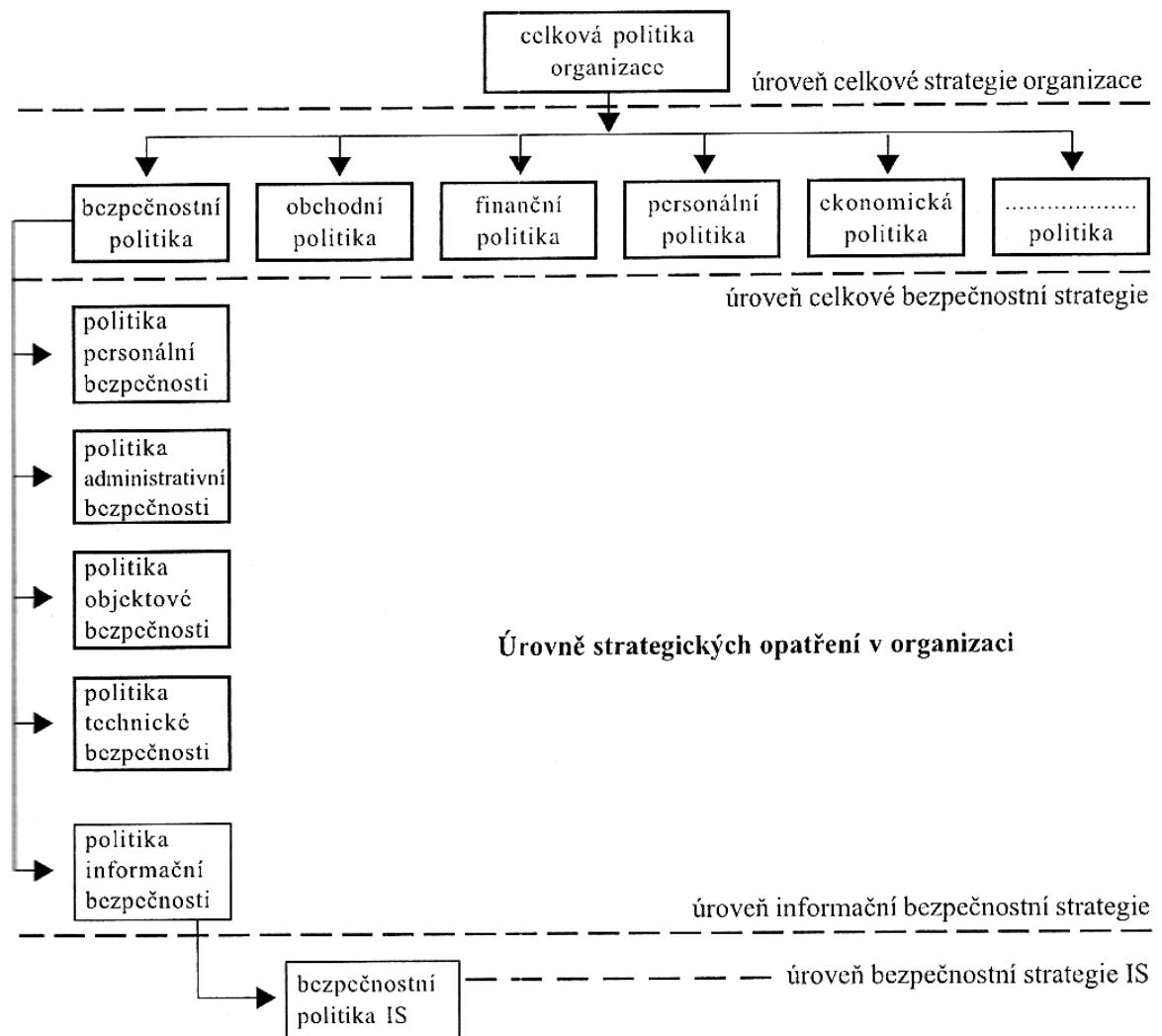
#### B) Charakterizuje

- Způsob a postupy řešení ochrany bezpečnosti firmy
- Časové podmínky řešení
- Finanční podmínky řešení
- Zásady havarijního plánování a řešení incidentů
- Způsoby zabezpečení ochrany bezpečnosti firmy
- Metody a způsoby řízení, organizace, koordinace a kontroly zajištění ochrany bezpečnosti organizace [2]

## 6.6 Bezpečnostní politika informačních systémů

Současné požadavky na ochranu informací jsou tak vysoké, že informační systémy, které nejsou provozovány s podporou automatizace, nejsou s to je naplnit. Zúžíme tedy pojem v tomto případě pouze na ty systémy, jejichž podstatu tvoří počítačový systém a jeho jednotlivé komponenty. Z pohledu existence a fungování IS v organizaci je rozhodně žádoucím stavem bezpečnost IS. Jako každý bezpečnostní cíl organizace je i bezpečnost IS výsledkem řady činností organizace směřujících k jejímu dosažení a udržení. Jedná se o komplexní proces, který je poměrně složitý. V zajištění bezpečnosti IS organizace se setkáváme se všemi již známými dokumenty a přístupy, přesto specifika IS tyto dokumenty a přístupy značně modifikují. V případě bezpečnosti IS je výchozím bodem bezpečnostní politika. Stejně jako představuje v rámci komplexní bezpečnosti organizace bezpečnost IS jen část bezpečnostní problematiky, je i bezpečnostní politika IS částí celkové bezpečnostní politiky organizace. Na níže uvedeném obrázku vidíme názorně graficky nadřaze-

nost celkové politiky organizace nad politikou bezpečnostní, která byla uvedena v předchozích částech.



Obr. 13 Vztah bezpečnostní politiky a celkové politiky organizace <sup>22</sup>

Základním východiskem pro bezpečnost organizace je celková politika (strategie) organizace. Celková bezpečnostní politika organizace je nejobecnějším vyjádřením nejzákladnějších principů zásad a prostředků k zajištění bezpečnosti organizace. Tato celková bezpečnostní politika se stává východiskem pro politiku informační bezpečnosti organizace. Pojmem informační bezpečnost organizace rozumíme veškerá bezpečnostní opatření sloužící k ochraně informací bez ohledu na způsob jejich zpracování a uložení (bez ohledu, zda je

<sup>22</sup> Převzato z: BRABEC, František a kolektiv. *Bezpečnost pro firmu, úřad, občana*, Praha, Public History, 2001, ISBN 80-86445-04-6.

informace uložena na papíře, v elektronické podobě či jinak). Politika informační bezpečnosti organizace je východiskem pro formulování bezpečnostní politiky IS v organizaci. [3]

### 6.6.1 Cíle bezpečnostní politiky organizace

Cílem bezpečnostní politiky IS je zajistit bezpečnost fungování informačních systémů používaných v organizaci s ohledem na bezpečnost informací vstupujících do tohoto systému, v něm obsažených a z něho vystupujících. Tedy předejít, eliminovat, minimalizovat či jiným způsobem překonat hrozby a rizika, kterým může být informační systém organizace reálně vytaven, aniž by organizace utrpěla významnou újmu. Obsah bezpečnostní politiky IS je velmi podobný celkové bezpečnostní politice organizace. Bezpečnostní politika IS musí řešit tyto otázky:

- Cíl bezpečnostní politiky IS
- Popis informačního systému a hodnocení jeho významu pro fungování organizace
- Legislativní východiska
- Definovat kategorie významu informací
- Definovat možné hrozby a rizika působící na IS
- Zásady personální politiky týkající se IS
- Zásady organizačně administrativních (režimových) opatření platných pro IS
- Technicko-provozní zabezpečení IS
- Politiku zálohování dat
- Definovat bezpečnostní služby, které má IS splňovat
- Řešit obnovu IS v období pro případ havárií
- Určit metodiku řešení krizí a mimořádných situací atd.

Komplexní řešení bezpečnosti IS organizace představuje provedení:

- Komplexní bezpečnostní expertizy informační bezpečnosti organizace (nebo komplexní expertizy IS), v rámci které bude provedena
- Celková analýza IS (analýza východisek, zdrojů a prostředí, popis IS atd.)

- Analýza rizik
- Formulace alternativ řešení
- Definování bezpečnostní politiky IS
- Projekt bezpečnosti IS a jeho realizace

### 6.6.2 Kritéria bezpečnostní politiky informačních systémů

Jedním ze základních kritérií IS je, aby systém vyhovoval podmínkám stanoveným obecně platnými právními předpisy, technickými normami a obecně užívanými standardy, pokud existují. Prolínání evropského a tuzemského prostoru je patrné na úpravách stávajícího právního systému státu legislativám Evropské Unie, které vždy bohužel neznamenaají změnu k lepšímu. My se však budeme zabývat oblastí počítačových technologií a informačních technologií. Pro analýzu bezpečnosti IS a pro rizikovou analýzu jsou dnes dostupné např.:

- TCSEC – jde o tzv. Oranžovou knihu (Orange Book) – definovaná kritéria stanovují jednotný soubor základních požadavků a vyhodnocení tříd pro určení efektivity kontroly bezpečnosti vestavěné do systémů automatizovaného zpracování dat
- ITSEC – zde je definován pojem hodnocený předmět. Definováno je 7 tříd v závislosti na míře záruky a dále deset tříd dalších. Dle dosažených výsledků hodnotitel vydá certifikát
- CRAMM (CCTA) – pochází z Velké Británie a je metodou analýzy rizik. Metoda odlišuje dvě základní aktivity – analýzu rizik a zvládnání rizik

Smyslem bezpečnostní analýzy IS je navrhnout bezpečnostní funkce IS při současném respektování možností organizace (zejména finančních). Nejdůležitější část této analýzy je analýza rizik.

### 6.6.3 Analýza rizik informačních systémů

Umožňuje zformulovat návrh protiopatření, tj. zvládnání rizik, které vliv rizik eliminují, nebo minimalizují. Hodnotitelé bezpečnosti IS, zvláště ti, co vypracovávají analýzu rizik, musí mít vysokou odbornost. Riziková analýza jako taková se provádí často na základě empirických poznatků o bezpečnostní problematice v informačních systémech. Každá chyba při analýze rizik se projeví chybou v celkovém návrhu bezpečnostních opatření. Rizika mohou být neadekvátní k opatřením v tom, že budou předimenzována, nebo podceněna.

Bezpečnostní analýza IS sleduje tři hlavní cíle: důvěrnost, integritu a dostupnost informací. Důvěrnost informací je zajišťována ochranou informací proti nepovolanému přístupu. Integrita je zajištěna ochranou proti neoprávněné modifikaci, pozměnění, zničení, změně nebo vymazání informace. Dostupnost jako poslední cíl znamená dostupnost informací při výpadku informačního systému včetně účinnosti havarijních postupů. K zajištění těchto hlavních cílů bezpečnostní analýzy IS je nutné provést analýzu:

- Řízení přístupu k informacím a komponentům IS
- Ochrany dat před neoprávněnou modifikací
- Ochrany IS před kriminálními skutky
- Ochrany před počítačovou infiltrací
- Ochrany personálu, know-how a autorských práv

Velmi důležitým prvkem v procesu zabezpečení IS je i hodnocení bezpečnosti IS. Jde o porovnání bezpečnostní úrovně IS s danými kritérii. Tento proces má dvě fáze:

- Certifikaci, která představuje porovnání bezpečnostního projektu IS s bezpečnostní politikou IS a potvrzuje se jí, že IS dosahuje požadovaných výsledků. Certifikace je současně jedním z podkladů pro akreditaci
- Akreditace je ve své podstatě administrativní proces, kdy orgán odpovědný za provoz IS prohlásí, že IS je schválen pro zpracování informací dle zadávacích, provozních a řídicích podmínek [7]

Součástí bezpečnostního procesu IS je písemný dokument – bezpečnostní směrnice, která představuje komplex pravidel pro bezpečné užívání IS v praxi. Ve směrnici musí být jednoznačně stanoveno:

- Kdo zodpovídá za konkrétní druhy bezpečnosti IS na pracovišti organizace
- Chování uživatelů při práci s IS
- Oprávnění přístupu uživatelů k informacím v IS
- Pořizování a vedení záznamů a písemností v souvislosti s užíváním IS

- Antivirová opatření
- Přístupová matice<sup>23</sup>
- Postupy při vytváření nových uživatelských účtů a rušení neplatných
- Činnost při haváriích
- Další (dílčí) směrnice, vyžaduje-li si to situace

Problematika bezpečnosti IS je nesmírně širokou oblastí. Z nejobecnějšího úhlu pohledu pro ni platí totéž, co pro bezpečnost organizace jako celku. Díky složitosti a neustálému progresu informačních technologií se neustále vyvíjí a klade stále náročnější požadavky na odbornost těch, kteří ji zajišťují. V souvislosti s komerční bezpečností jde o specifickou oblast, kterou se zabývají vysoce kvalifikovaní odborníci a odborné firmy.

---

<sup>23</sup> Tabulka s vyznačením oprávněných subjektů a jejich oprávnění k práci s určitým objektem IS a povolený způsob této práce.

## 7 BEZPEČNOSTNĚ TECHNICKÉ POŽADAVKY NA BEZPEČNOST ORGANIZACE

Bezpečnostně technické požadavky stanovují návod k zavedení systému vnitřního řízení bezpečnosti v podniku, bez ohledu na jeho velikost, druh aktivit, charakter atd. Bezpečnostně technické požadavky jsou určeny pro podniky a podnikatele podléhající dozoru státního odborného dozoru ve smyslu ustanovení §3 zákona č. 174/1968 Sb.<sup>24</sup>, ve znění pozdějších předpisů. [19]

### 7.1 Termíny a terminologie

**Audit** – bezpečnostní audit je nástroj řízení zahrnující systematické, dokumentované, periodické, objektivní a odborné posouzení a vyhodnocení zavedeného systému řízení bezpečnosti ve sledované oblasti. Do této oblasti spadá systém prevence rizik provozních nehod a nehodových událostí a ochrany životního prostředí včetně legislativního zázemí. Cílem je ověřit funkce systému řízení bezpečnosti v podniku. Realizuje se formou vnějšího (externího), nebo vnitřního (interního neboli vlastního) auditu. Výstupní dokument auditu je závěrečná zpráva o nálezech a závěrech. [11]

- Vnější audit – prováděný odbornými pracovníky nezávislé organizace, nebo orgánu
- Vnitřní audit – prováděný odbornými pracovníky nebo odborným útvarům vlastního podniku (bezpečnostní management)

**Bezpečnost práce** – ochrana života a zdraví osob, životního prostředí a majetku před negativními účinky pracovních procesů a všech dalších činností, které s pracovními procesy přímo nesouvisí, ale ve svém důsledku mohou toto ohrožení způsobit.

**Pracoviště** – jsou všechna místa, kde se zaměstnanci nacházejí, nebo kam se ubírají k výkonu své práce. Jsou to také místa, kde se zdržují s vědomím zaměstnavatele a která podléhají přímému nebo nepřímému dozoru.

---

<sup>24</sup> Zákon č. 174/1968 Sb. V platném znění O státním odborném dozoru nad bezpečností práce.

**Předpisy** – právní a ostatní předpisy k zajištění bezpečnosti a ochrany zdraví při práci. Mezi tyto předpisy řadíme:

- Předpisy na ochranu života a zdraví
- Předpisy hygienické a protiepidemické
- Předpisy o bezpečnosti technických zařízení a technické normy
- Dopravní předpisy
- Předpisy o požární ochraně
- Předpisy o zacházení s hořlavinami, výbušninami, zbraněmi, radioaktivními látkami, jedy a jinými látkami, které škodí zdraví

Za předpisy k zajištění bezpečnosti a ochrany zdraví při práci se považují i pravidla o bezpečnosti a ochraně zdraví při práci vydaná ústředními orgány, nebo zaměstnavateli v dohodě s příslušnými orgány.

**Vnitřní kontrola** – plánovaná, organizovaná, soustavná kontrolní činnost, přizpůsobená a realizovaná tak, aby bylo zajištěno dodržení požadavků a předpisů - v rámci všech aktivit na všech úrovních a fázích činnosti podniku. Vnitřní kontrolu provádí každý vedoucí zaměstnanec na pracovišti, za které odpovídá.

**Bezpečnostní politika** – písemné vyjádření snahy vrcholového vedení podniku zajistit bezpečnost, přijmout závazky v oblasti bezpečnosti a zviditelnit tyto aktivity jak uvnitř, tak vně podniku.

**Skoronehoda** – skutečná událost, která nastala, při níž mohlo dojít k ohrožení života a zdraví, majetku (případně současně), ale pouze náhodnou shodou okolností k tomuto následku nedošlo.

**Bezpečnostní management** – je efektivní, samoregulující se systém, zajišťující integrované řízení bezpečnosti v podniku. Realizuje jej vedení podniku (podnikový management) na základě bezpečnostní politiky za spoluúčasti všech zaměstnanců.

**Riskmanagement** – systém řízení (omezování) rizik, který zahrnuje činnosti při identifikaci, kvantifikaci a eliminaci rizik nebo snižování rizik na přijatelnou úroveň.

**Výchova** – vzdělávání zaměstnanců, které zahrnuje vstupní, periodické a speciální školení:

- Vstupní školení – proškolení zaměstnanců při nástupu do zaměstnání před jejich pověřením výkonem určité práce z příslušných bezpečnostních předpisů a zásad bezpečného chování na pracovišti, a to v celém rozsahu pracovního procesu, tj. proškolení z právních a ostatních předpisů k zajištění BOZ<sup>25</sup> při práci (ve smyslu § 273<sup>26</sup> zákoníku práce č. 262/2006 Sb.), z předpisů týkajících se ochrany životního prostředí a předcházení haváriím. [25]
- Periodické školení – je pravidelně se opakující školení v termínech, stanovených předpisy, nebo zaměstnavatelem.
- Speciální školení – proškolení a praktické zacvičení specialistů v oblasti jimi vykonávaných speciálních činností. [4]

## 7.2 Zásady systému vnitřního řízení bezpečnosti podniku a prvky tohoto systému

**Zavedení systému** – potřeba zavedení účinného a účelného systému řízení bezpečnosti a ochrany zdraví, životního prostředí a majetku společnosti vzniká okamžikem rozhodnutí řídit hospodárně lidské zdroje a zavést takový dokumentovaný soubor řídicích a kontrolních prvků, které umožní jak jejich racionální využití, tak i maximální možné vyloučení jejich selhání, bez ohledu na to, jakým způsobem jsou do ekonomické aktivity zapojeny. Pro řízení platí stejné zásady jako pro řízení ekonomických aktivit. Řízení bezpečnosti

---

<sup>25</sup> Bezpečnost a ochrana zdraví.

<sup>26</sup> (1) Plněním pracovních úkolů je výkon pracovních povinností vyplývajících z pracovního poměru a z dohod o pracích konaných mimo pracovní poměr, jiná činnost vykonávaná na příkaz zaměstnavatele a činnost, která je předmětem pracovní cesty.

(2) Plněním pracovních úkolů je též činnost konaná pro zaměstnavatele na podnět odborové organizace, rady zaměstnanců, popřípadě zástupce pro oblast bezpečnosti a ochrany zdraví při práci nebo ostatních zaměstnanců, popřípadě činnost konaná pro zaměstnavatele z vlastní iniciativy, pokud k ní zaměstnanec nepotřebuje zvláštní oprávnění nebo ji nevykonává proti výslovnému zákazmu zaměstnavatele, jakož i dobrovolná výpomoc organizovaná zaměstnavatelem.

musí být přijato jako organická součást řízení všech aktivit podniku a mělo by být chápáno jako ekonomická, etická a humánní součást přístupu podnikatele k řešení všech činností. Hovoříme tedy o soustavné činnosti, a tedy řízené, zajišťované a vyžadované vrcholovým vedením podniku.

**Organizace systému** - Prvky řízení vycházejí z vnitřního uspořádání a potřeb podniku a pokrývají jeho veškeré aktivity.

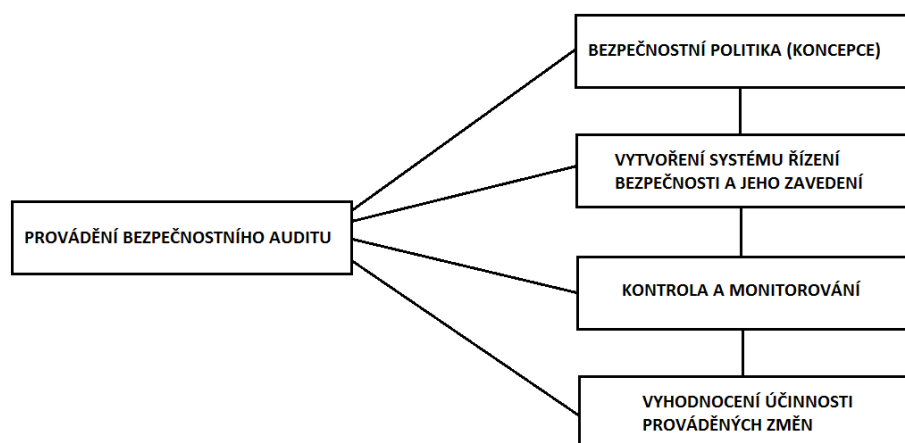
- Je nutné vytvořit optimální organizační strukturu.
- Musí být vytvořen systém informací a zdrojů informací.
- Musí být vytvořena soustava činností, pravomocí a systém odpovědnosti.
- V systému řízení bezpečnosti musí být zahrnuty všechny osoby, kterých se aktivity podniku týkají (dodavatelé, subdodavatelé, odběratelé, návštěvníci, veřejnost atd.).
- Systém řízení ve všech fázích musí být dokladovatelný.
- Požadavky musí být konkrétní a výsledky měřitelné.
- Systém řízení má být zaveden tak, aby jej bylo možno integrovat s ostatními potřebami řízení<sup>27</sup>.

#### **Ostatní zásady**

- Musí být zajištěna aktivní účast zaměstnanců podniku.
- Musí být vytvořen systém školení, systém výcviku, vhodné a účinné formy motivace jednotlivých zaměstnanců na všech úrovních.
- Vyžadování dodržování stanovených předpisů, opatření, postupů a zásad. Musí být uplatňováno při všech příležitostech.
- Jednotlivé prvky vnitřního řízení bezpečnosti v podniku musí být vzájemně provázány. [4]

---

<sup>27</sup> Například ISO 9000, prevence závažných havárií, atd. [27]

Obr. 14 Prvky vnitřního řízení společnosti<sup>28</sup>

### 7.3 Úkoly vedení podniku při zavádění systému vnitřního řízení bezpečnosti

Vedení společnosti spolu s bezpečnostním managementem představuje základní složku tvorby systému bezpečnosti a nese za tuto problematiku plnou odpovědnost. Musí se proto s požadavky systému řízení bezpečnosti ztotožnit a realizovat je. Má následující úkoly:

- Formulování bezpečnostní politiky (koncepce).
- Rozhodnutí o ekonomickém zajištění bezpečnostních aktivit.
- Vytvoření organizační struktury, systému vnitřní (vertikální i horizontální) i vnější komunikace (obchodní vztahy, vztah k veřejnosti, samosprávě a státním orgánům).
- Vytvoření vnitropodnikových aktů.
- Stanovení konkrétní odpovědnosti a odpovídajících pravomocí.
- Zavedení vlastní legislativy v návaznosti na dotčené předpisy.
- Stanovení způsobu získávání, třídění a vyhodnocování informací.

---

<sup>28</sup> Převzato z: ELBEL, Jaromír. *Systém vnitřního řízení bezpečnosti v podniku*. Část 1, Metodický návod k zavedení systému. Praha, Český úřad bezpečnosti práce, 1998, ISBN 80-901654-5-1.

- Zajištění motivace a angažovanosti zaměstnanců.
- Stanovení požadavků na pracovní místo a na pracovníka (vč. mezních hodnot).
- Formulování cílů a stanovení dlouhodobých a krátkodobých úkolů.
- Vytvoření nástrojů pro prosouzení ekonomické náročnosti přijatých opatření.
- Zavedení norem řízení, programů školení a vzdělávání, výcviku, bezpečných pracovních technologických postupů, postupů pro povolání prací.
- Stanovení rozsahu vnitřní kontroly.
- Stanovení systémů umožňujících monitorování provedených opatření.
- Hlášení, šetření a evidence nehodových událostí (včetně skoronehod).
- Zavedení vnitřní kontroly.
- Zavedení kontroly obvyklých a neobvyklých provozních stavů, stanovení mezních hodnot (včetně nutných opatření), stanovení provádění kontrol, zkoušek a revizí včetně dokumentování a evidence.
- Zavedení kontroly kvality.
- Zavedení systémů umožňujících monitorování provedených opatření.
- Zavedení systémů průběžného hodnocení rizik a provádění nápravných opatření.
- Zavedení systému pravidelných auditů a dalších kontrolních mechanismů.
- Tyto požadavky je nutné dokumentovat v přiměřeném rozsahu písemnou formou.

Uvedené důvody zahrnují vlastní činnost podniku, dodávku služeb, prodej zboží, údržbu, opravy, poskytování služeb včetně skladování a manipulace se zbožím, likvidaci odpadu, možné vlivy na okolí. Jak již bylo řečeno, tato opatření se dotknou jak zaměstnanců, dodavatelů, subdodavatelů, tak i odběratelů, návštěvníků, veřejnosti, atd.

### **7.3.1 Koordinace činností na všech stupních řízení včetně koordinace dodavatelské činnosti**

Koordinace činností a stanovení odpovědností vychází ze stanovených úkolů pro vedení podniku tak, jak je uvedeno v předchozí pasáži, z organizačního uspořádání a členění podniku. Je nutno sledovat vertikální a horizontální vazby mezi jednotlivými útvary, případně odpovědnými zaměstnanci. Dále je zapotřebí rozlišovat stupně řízení a jeho počet včetně

rozsahu případné vnitropodnikové kontroly. Zde platí zásada, že ten kdo řídí, musí zodpovídat, musí být motivován a musí mít nástroje a pravomoci na prosazování stanovených požadavků. Jednotlivé činnosti a odpovědnosti na sebe musí optimálně navazovat a jsou odpovídajícím způsobem rozděleny mezi:

- Vrcholové vedení společnosti (jednatel)
- Střední řídicí úroveň (např. ředitel oddělení)
- Základní řídicí úroveň (např. mistr, vedoucí pracovní skupiny)
- Odborné pracovníky (bezpečnostní, revizní, požární techniky, případně další specialisty)
- Zaměstnance

Návaznost je zajištěna nejen při činnostech uvnitř podniku, ale musí odpovídat i vztahům navenek. Uvedeme si příklad: Pracovník odpovědný za určitou činnost uvnitř podniku musí vystupovat tímto způsobem i vůči dodávkám, případně subdodávkám externím dodavatelem, to znamená, že jeho odpovědnost nesmí být zpochybněna, nebo omezena obchodní, nebo obdobnou smlouvou. [4]

### 7.3.2 Kontrolní činnosti a audit

**Průběžná kontrola** – dodržování předpisů a stanovených zásad jako soustavná činnost, která je nedílnou součástí plnění každodenních povinností. Je prováděna všemi zaměstnanci, včetně vedoucích na všech stupních řízení ve stanoveném rozsahu.

**Vnitřní kontrola** – plánovaná organizovaná činnost přizpůsobená a udržovaná tak, aby bylo důsledně prověřeno a zajištěno dodržení požadavků příslušných předpisů. Musí pokrýt všechny aktivity podniku na všech úrovních a fázích činností.

**Inspekce** – systém řízení bezpečnosti v podniku, je prováděna kontrolním orgánem z jeho vlastního podnětu, nebo na žádost podniku. Cílem je:

- Ověřit úroveň zavedeného systému řízení bezpečnosti.
- Upozornit na nedostatky v systému.
- Prověřit naplnění zásad stanovených systémem (povinnosti a odpovědnosti stanovených jednotlivým vedoucím pracovníkům i řadovým zaměstnancům).

Vzájemná provázanost výše uvedených kontrolních činností spočívá v tom, že

- Výsledky jednotlivých průběžných kontrol slouží jako podklad pro provádění vnitřní kontroly.
- Výsledky vnitřní kontroly by měly sloužit jako jeden z podkladů pro zpracování zpráv o auditech.

**Audit** – provádí se vždy v souvislosti se zavedením systému řízení bezpečnosti podniku, dále v pravidelných intervalech, případně při výrazném, nebo trvalém zhoršení některých sledovaných ukazatelů. Z toho plyne i stanovení rozsahu a záměru auditu podle toho, co vyvolalo potřebu jej provést.

### **Vzájemné vztahy subjektů**

Subjekty účastníci se auditu, nebo kontroly musí dodržovat následující zásady:

- Maximální spolupráci mezi kontrolovaným a kontrolním subjektem.
- Zachování mlčenlivosti<sup>29</sup> o skutečnostech, které auditorská nebo kontrolní organizace zjistí, a to zejména pokud se týká výrobních nebo obchodních tajemství.

### **7.3.3 Rozsah vnitřní kontroly na pracovišti**

Vnitřní kontrola na daném pracovišti by měla zajistit, že ekonomické činnosti na pracovišti jsou plánovány, prováděny, udržovány a kontrolovány v souladu s požadavky předpisů. Vnitřní kontrola je součástí integrovaného systému řízení. Je prováděna a dokumentována tak, aby bylo možno provádět měřitelné a porovnatelné vyhodnocení. Vzhledem k tomu, že vnitřní kontrolu na daném pracovišti provádí vedoucí zaměstnanec, který je zároveň za ekonomické výsledky zodpovědný, lze velmi snadno konkrétně dokumentovat dosažený stav a případně okamžitě zjednat nápravu. Kontrolní seznam pro provádění vnitřní kontroly je nutno zpracovat podle daného rozsahu činností a stanovených cílů a úkolů, například dle níže uvedených otázek. Každý bod je nutno vyhodnotit například procentuálně:

- 0 – 20%      stav naprosto nedostatečný, nevyhovující
- 21 – 40 %    stav nedostatečný, závažné nedostatky zásadního charakteru
- 41 – 60 %    stav nedostatečný, mnoho závad

---

<sup>29</sup> Vůči třetí osobě.

- 61 – 80 %      menší závady
- 81 – 99%      nepodstatné závady
- 100 %          bez závad

Vyhodnocení – provádí každý vedoucí zaměstnanec na pracovišti jako nedílnou součást vnitřní kontroly. Pro jednoduchost a rychlost je vhodné použít připravené kontrolní seznamy, na základě kterých je možno nejen kontrolu na daném pracovišti provést, ale zaměstnanec si sám může dosaženou úroveň okamžitě vyhodnotit. Je žádoucí, aby při každém následujícím hodnocení byl stav lepší. Zlepšení musí být prokazatelné a měřitelné.

Součástí vyhodnocení vnitřní kontroly je uvedení závad, jejichž řešení není v pravomoci a možnostech vedoucího pracovníka, který kontrolu provedl. To znamená, že k jejich řešení je z hlediska svých pravomocí kompetentní jemu nadřízený pracovník. Pravidla lhůty pro vyhodnocení a nápravu nedostatků volí podnik způsobem, který si stanoví podle zásad uvedených v bezpečnostně technických požadavcích.

V projektové části je vypracován kontrolní seznam pro provedení vnitřní kontroly v podobě tabulky a hodnocení (vyhovuje × nevyhovuje), má formu jednoduchého, avšak účinného prostředku pro dosažení celkové bezpečnosti ve firmě.

### **Struktura auditu BOZP**

Audit má prověřit především stav na úseku

1. Koncepce bezpečnosti, ochrany zdraví a životního prostředí
2. Odpovědnosti vrcholového vedení společnosti
3. Cílů
4. Organizačního zabezpečení
5. Technického zabezpečení
6. Ekonomického zabezpečení
7. Bezpečnostních instrukcí
8. Povinností a odpovědností
9. Komunikace mezi jednotlivými subjekty
10. Identifikace zdrojů rizik

11. Hodnocení rizik
12. Stanovených opatření přijatých na základě identifikace a hodnocení rizik
13. Prevence havárií
14. Kvalifikace
15. Výchovy a výcviku
16. Spolupráce
17. Motivace
18. Zdravotní péče
19. Osobních ochranných prostředků
20. Kontroly a monitorování

Společnost si po dokončení bezpečnostního projektu pozve externí bezpečnostní audit, který prověří tyto okruhy:

- Zjistit, zda objekt pracuje v bezpečnostním režimu, tj. zda existuje bezpečnostní politika a zda jsou zpracovány bezpečnostní plány ochrany.
- Zjistit, zda je zaveden systém jakosti a jak je koncepčně vystavěn.
- Zjistit, zda systém jakosti, jeho jednotlivé prvky procesu výroby či služby a pracovníci odpovídají požadavkům příslušných norem, směrnic, nařízením a jak jsou tyto požadavky realizovány.
- Jaká jsou v objektu realizována režimová opatření.
- Jaká je v objektu nasazena bezpečnostní a protipožární technika.
- Zjistit, zda existují havarijní plány, jaká je jejich funkčnost a aktualizace.
- Ověřit, zda reálné procesy probíhají v souladu s dokumentovaným systémem stále a za všech okolností.
- Ověřit, zda je implementace systému jakosti účinná, tj. splní svůj základní cíl, čili zda vytváří podmínky pro splnění požadavků zákazníka.
- Poskytnout jasnou a zřejmou formulaci zjištěných závad doložených objektivními důkazy

- Podat návrhy nápravných opatření a doporučení ke zlepšení s konkrétním termínem odstranění, jasnou a adresnou personální odpovědností výkonného pracovníka a odpovědného manažera.

Závěr bezpečnostního auditu musí být jednoznačný, bezvýhradný a nezavádějící. Nesmí připouštět několikový výklad.

Závěr se vyjadřuje ve třech rovinách:

- AT – vyhovuje bez výhrad
- A – vyhovuje podmíněně
- B – nevyhovuje [12]

Charakteristiky jakosti výrobku lze rozčlenit do následujících kategorií:

- Technické – chemické, fyzikální, nebo biologické vlastnosti
- Ovlivňující náročnost při provozování výrobku a jeho vlivu na okolí – bezporuchovost, ovladatelnost, bezpečnost, atd.
- Estetické – vzhled výrobku, módnost
- Logistické – dostupnost, dodací služby, apod.

K charakteristikám jakosti služeb patří:

- dostupnost (čekací doba, vzdálenost od bydliště zákazníků, geografická poloha, provozní doba)
- komunikace (informovanost zákazníka, umění mu naslouchat)
- kompetence personálu (aplikace znalostí na specifickou službu)
- zdvořilost personálu
- věrohodnost (tradice podniku, jeho záruky)
- spolehlivost výkonu služby
- porozumění potřebám zákazníka

## **II. PRAKTICKÁ ČÁST**

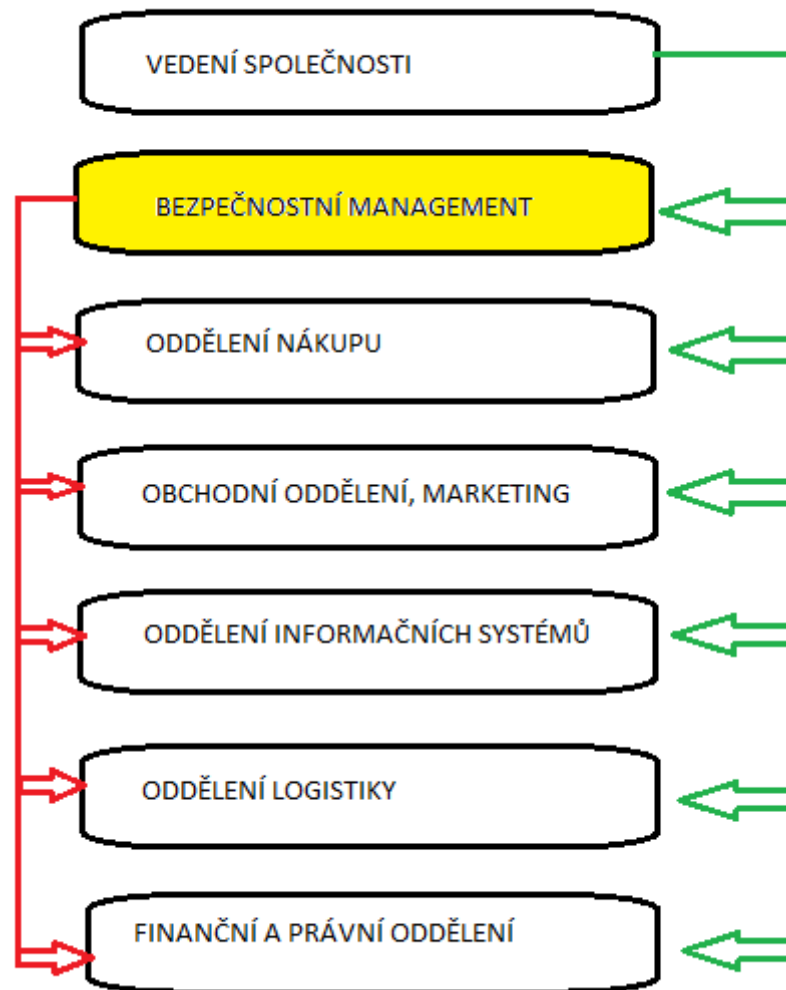
## 8 ZAVEDNÍ BEZPEČNOSTNÍ POLITIKY ORGANIZACE

V této části diplomové práce rozebereme všechny dosud zjištěné poznatky o bezpečnostním plánování a operací s ním souvisejících v praxi.

### 8.1 Profil společnosti

Budeme hovořit o fiktivní společnosti AZ Elektro s. r. o. Společnost funguje od roku 2013, je vlastněna majitelem Janem Novákem. Tato společnost se specializuje na prodej spotřební elektroniky, se zaměřením zejména na internetový obchod. Vlivem expanze společnosti na trh se management rozhodl o rozšíření skladových prostor, kompletní změnu informačního systému a zlepšení dosavadních služeb. Společnost chce reagovat na stále se zvyšující nároky nakupujících zákazníků a cílem by měla být v první řadě spokojenost zákazníka z pohledu výběru zboží, dobré kvality zboží a dostupné ceny. Tyto zavedené zásady by měly zajistit dobrou konkurenceschopnost a stabilitu společnosti. AZ Elektro z jedné poloviny nakupuje zboží od velkoobchodníků a druhou polovinu zboží pod privátní značkou nechává vyrábět přímo pro sebe a je tedy výhradním dodavatelem pro tyto značky spotřebičů. S tímto přístupem je spojena řada nejen logistických a administrativních procesů, jejichž dobrá funkce je pro společnost klíčová. Z tohoto důvodu se tedy společnost rozhodla ke zpracování firemní strategie, na jejichž základech hodlá odvíjet svou další činnost. Podnik se dostal do fáze, kdy dosavadní postupy a plány nebyly dost jasně definovány a nebyly tedy adekvátní k současné situaci, kdy společnost zaznamenala vývoj nárůstu tržeb a zvýšení obrátu. Jde o řízení firmy z pohledu efektivního nastavení pravidel, vymezení celkové vize společnosti, určení odpovědností a zpracování kvalitní bezpečnostní politiky, jež bude úzce spjata s celkovou firemní strategií.

## 8.2 Struktura společnosti



Obr. 15 Struktura společnosti <sup>30</sup>

### 8.2.1 Vedení společnosti

**Vedení společnosti** se skládá, z jednatele a dalších dvou členů vedení. První z nich zastává funkci personálního ředitele, druhý člen vedení zastupuje jednatele společnosti v jeho nepřítomnosti. Rozhodovací pravomoci zásadního charakteru má však pouze jednatel – všechny sekce jsou podřízené včetně bezpečnostního manažera, který je přímo odpovědný vedení společnosti. Sleduje obchodní výsledky podniku, jeho profit a rovněž aktuální reporty ze všech oddělení. Aktivně se podílí na všech inovacích, snaží se firmu neustále po-

<sup>30</sup> Obrázek vlastní

souvat dále. Součástí vedení je též personální oddělení, které obstarává veškerou administrativu v řízení lidských zdrojů. Po boku vedení mají svou kancelář asistenti plnící zároveň úlohu oddělení vnější komunikace.

### 8.2.2 Bezpečnostní management

**Bezpečnostní management** je zodpovědný za dodržování bezpečnostní politiky a všech pravidel jak pro informační, tak i technickou bezpečnost. Ve společnosti má na starosti bezpečnostní školení, zpracovává krizové a havarijní plány, objednává a dohlíží nad převozem hotovosti z poboček, má právo kontrolovat činnost všech oddělení. Tato struktura funguje na bázi facility managementu.<sup>31</sup> Řídí sekci, která je přímo jemu podřízená – správu majetku a služeb společnosti; ta dohlíží nad provozem společnosti, údržbou nebo vozovým parkem a zajišťuje evidenci všech služeb a energií. Úzce spolupracuje s finančním a právním oddělením, kde dochází ke zpracování všech uzavřených smluv s externími dodavatelskými společnostmi. Pro oddělení nákupu a obchodní oddělení eviduje a sleduje dodržování bezpečnostních procedur při nakládání s dokumenty, jako jsou smlouvy s dodavateli, tvorba cen a další neveřejné informace jako například nákupní ceny, obchodní marže, nebo statistiky prodeje. Pořádá školení bezpečnosti práce a ochrany zdraví při práci. Je pověřen vedením společnosti ke komunikaci s bezpečnostními složkami státu.

### 8.2.3 Oddělení nákupu

**Oddělení nákupu** zajišťuje objednávání a nákup nového zboží. Úzce komunikuje s dodavateli jak tuzemskými tak zahraničními. Spolupracuje též s oddělením logistiky. Analyzuje nabídky dodavatelů, při větších objednávkách kooperuje s obchodním oddělením a vedením společnosti. Má na starosti nákup zboží od velkoobchodů. Zajišťuje výrobu zboží vlastních značek v Číně. Spolupracuje s oddělením logistiky, kde řeší otázky tuzemské dopravy a forwardingu ze vzdálených zemí. S právním oddělením konzultuje smlouvy s dodavateli.

---

<sup>31</sup> Facility management (EN15221) [31] je multioborová disciplína, která se zabývá řízením podpůrných činností firmy. Mezi podpůrné procesy tak můžeme zařadit např. správu ploch, správu a údržbu budov, investičního oddělení, správu vozového parku, řízení energií, řízení externích vztahů, evidenci majetku, řízení nájmů atd. [30]

#### 8.2.4 Obchodní oddělení

**Obchodní oddělení, marketing** se stará o propagaci zboží, reklamu, ale v neposlední řadě také spravuje agendu kamenné pobočky (showroomy, výdejní místa). Jedná se zde o zajištění včasného dodání zboží, spolupráce je vázána na oddělení logistiky. Společně s oddělením nákupu tvoří cenovou politiku, do které má co říci i vedení společnosti. Sleduje marže společnosti, konzultuje tvorbu cen s nákupním oddělením. Zajišťuje průzkum trhu a konkurence.

#### 8.2.5 Oddělení informačních systémů

**Oddělení informačních systémů** spravuje kompletní infrastrukturu týkající se provozu serverů, firemního informačního systému, na který je navázán skladový systém, e-shop, registrace uživatelů, plní službu Helpdesku, kde pomocí vzdáleného přístupu řeší nepřetržitě všechny situace týkající se informačních systémů. Spolupracuje s bezpečnostním manažerem, dbá o dodržování pravidel informační bezpečnosti, bezpečnostní management sleduje, zda dodržují všechna stanovená pravidla v bezpečnostní politice informačních systémů.

#### 8.2.6 Oddělení logistiky

**Oddělení logistiky** má na starosti tok zboží, komunikuje s dodavateli o přepravních podmínkách, dodacích termínech. Spravuje skladový systém, provoz skladu a inventarizaci zboží. Výsledek inventury předává bezpečnostnímu managementu k analýze. Pokud jsou nalezeny nedostatky, bezpečnostní management upravuje režimová opatření skladu. Zajišťuje též spolupráci s přepravními společnostmi. Nad dodržováním všech pravidel při smluvním styku s dopravci opět dohlíží bezpečnostní management. Oddělení logistiky rovněž zajišťuje import zboží přes dopravní společnosti přímo z továren na centrální sklad nebo přes přístavy, kde je zboží v kontejnerech překládáno. Musí tudíž spolupracovat s celní správou. V neposlední řadě pak oddělení logistiky zajišťuje placený rozvoz objemného zboží přímo k zákazníkovi.

#### 8.2.7 Finanční a právní oddělení

**Finanční a právní oddělení.** Finanční oddělení se zabývá účetními transakcemi firmy, zpracovává podklady a faktury z nákupního a obchodního oddělení, zpracovává mzdy zaměstnanců dle podkladů personálního oddělení. Bezpečnostní management dohlíží nad dodržováním informační bezpečnosti na tomto úseku, podává podklady na zpracování fak-

tur za služby a dodavatelskou činnost, zejména v oblasti bezpečnosti. Právní oddělení kontroluje správnost podoby smluvních vztahů, sleduje aktuální změny v legislativě, právně zastupuje společnost ve všech směrech.

## **8.3 STRUKTURA BEZPEČNOSTNÍ POLITIKY ORGANIZACE**

### **8.3.1 Obecná ustanovení**

- Bezpečnostní politika společnosti AZ Elektro, s. r. o. ctí všechny zásady a normy uvedené v nadřazené obecné politice společnosti.
- Společnost AZ Elektro, s. r. o. je obchodní subjekt zabývající se prodejem spotřební elektroniky.
- Její základní pilíře a cíle bezpečnostní politiky jsou ochrana života, zdraví zaměstnanců a osob pohybujících se v prostorách společnosti.
- Dále mezi důležité hodnoty patří ochrana všech druhů majetku společnosti a životního prostředí.
- Mezi základní zásady společnosti patří transparentnost a firemní etika vůči veřejnosti.
- Důvěra zákazníka a jeho pozitivní pohled na společnost.
- Spokojenost zákazníka s výběrem a kvalitou zboží.
- Budování dobrých a spolehlivých vztahů mezi dodavatelskými společnostmi.
- Bezpečnostní politika je nadřazena všem provozním řádům, které z těchto bodů vycházejí a jsou vždy zformulovány pro danou činnost.
- Každý zaměstnanec je seznámen s úplným zněním a svým podpisem toto seznámení stvrzuje.

### **8.3.2 Oblast personální bezpečnosti**

- Každý zaměstnanec společnosti je k firmě loajální a vždy jedná dle svého nejlepšího vědomí za účelem naplnění všech cílů, které jsou zásadní pro tuto společnost.
- Cílem každého zaměstnance je minimalizace ztrát a maximalizace prosperity.

- Zaměstnanec dodržuje společenské minimum a etiketu při svém vystupování a svým chováním neporušuje pověst firmy.
- Každý zaměstnanec je při nástupu do zaměstnaneckého poměru a poté v pravidelných cyklech školen v oblasti bezpečnosti, ochrany zdraví při práci a požární bezpečnosti, která jsou v kompetenci bezpečnostního managementu.
- Pracovníci jsou školeni o problematice informační bezpečnosti.
- Každý zaměstnanec pracující s údaji týkající se firemního tajemství se závazně řídí aktuální legislativou – nový občanský zákoník č. 89/2012 Sb. § 504,<sup>32</sup> §2985.<sup>33</sup> [26]
- V případě, že se setká zaměstnanec s chováním svého kolegy, které je v rozporu s firemní či bezpečnostní politikou, ihned bez odkladu informuje svého nadřízeného nebo přímo kontaktuje bezpečnostního manažera.
- Pokud se zaměstnanec setká s jakoukoli nestandardní situací či situací, která překračuje hranici zákona, nezatajuje určité skutečnosti, zváží další postup, případně kontaktuje nadřízeného pracovníka.
- V případě porušení pravidel bezpečnostní politiky níže uvedených je zaměstnanec obeznám s tím, že zaměstnavatel může přistoupit dle závažnosti porušení

---

<sup>32</sup> Obchodní tajemství tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastníky zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení.

<sup>33</sup> Porušením obchodního tajemství je jednání, jímž jednatel sdělí, zpřístupní, pro sebe nebo pro jiného využije obchodní tajemství, které může být využito v soutěži a o němž se dověděl

a) tím, že mu tajemství bylo svěřeno nebo jinak se stalo přístupným na základě jeho pracovního poměru k soutěžiteli nebo na základě jiného vztahu k němu, popřípadě v rámci výkonu funkce, k níž byl soudem nebo jiným orgánem povolán, nebo

b) vlastním nebo cizím jednáním porušujícím se zákonem

k finančním sankcím, k rozvázání pracovního poměru a bude též spolupracovat s bezpečnostními složkami státu, bude-li si to žádat závažnost situace.

- Každý zaměstnanec se zavazuje k tomu, že nebude za žádných okolností šířit bez vědomí zaměstnavatele interní informace společnosti, jako jsou: osobní údaje zaměstnanců, obchodní výsledky společnosti, nákupní ceny zboží, informace o ztrátách. Dále nebude zveřejňovat bez vědomí vedení informace o smlouvách se zaměstnanci, zákazníky, dodavateli zboží a služeb, informace z oblasti účetnictví, fakturace a dalších neveřejných informací.
- Zaměstnanci nekomunikují v souvislosti se společností se zástupci médií a dalších informačních prostředků; k této komunikaci je výhradně určeno oddělení vnější komunikace.
- Personální oddělení zajišťuje centrální evidenci všech zaměstnanců společnosti ke zpracování jejich údajů za jednotlivými účely.
- Personální oddělení zpracovává za součinnosti příslušných správců (odpovědných osob) osobní údaje všech zaměstnanců a to po předchozím ověření identity v souladu se zákonem č. 101/2000 Sb. O ochraně osobních údajů [22]
- Personální oddělení zajišťuje komunikaci s Úřadem pro ochranu osobních údajů, ve spolupráci s bezpečnostním manažerem komunikuje s policií ČR a dalšími orgány státní správy, nebo samospráv ve věci ochrany neveřejných informací.
- Personální oddělení plní na základě rozhodnutí vedení oznamovací povinnost vůči Úřadu pro ochranu osobních údajů a rovněž žádá tento úřad o předání osobních údajů do zemí mimo EU.
- Každý zaměstnanec musí chránit zdraví své i zdraví druhých tím, že bude dodržovat všechna stanovená bezpečnostní a režimová opatření.
- Každý zaměstnanec bude používat ochranné pracovní pomůcky určené pro jednotlivé činnosti, každý vedoucí pracovník musí upozornit zaměstnance na správné dodržování předpisů, pokud vidí, že situace není v souladu s bezpečnostními požadavky.

- Personální oddělení je zodpovědné za vytvoření pracovních náplní jednotlivých pozic, kde jsou jasně popsány vztahy mezi nadřízeným a podřízeným zaměstnancem, příslušné kompetence, zodpovědnost a instrukce k určené pozici.
- Každé čtvrtletí je řešena otázka hodnocení a na konci každého kvartálu zaměstnanec dostane cíl, který za dané čtvrtletí naplňuje.

### 8.3.3 Oblast organizační

- Prostory společnosti AZ Elektro podléhají režimovým opatřením.
- Tento prostor se dělí na vnitřní a vnější (přílehlé okolí) a z hlediska využití se tyto prostory dělí administrativní a skladové, specifickou formou prostor jsou prodejny a výdejní místa, která mají status prostor skladových.
- Pro každý druh prostředí (administrativního či skladového) je vytvořen provozní řád, který vychází z bodů bezpečnostní politiky a je přímo vytvořen pro danou oblast. Tyto řády jsou závazné pro všechny osoby pohybující se v daných prostorech.
- Existují prostory, kde je vymezen přístup výhradně osobám, které mají k tomuto vstupu pověření.
- Každá osoba vcházející do skladu je povinna se před vstupem zaregistrovat u bezpečnostního pracovníka, tato povinnost platí pro administrativní budovu a sklad.
- Každá osoba vycházející z prostor skladů prochází bezpečnostním rámem a na vyzvání strážného vykonávajícího službu se podrobí fyzické kontrole; tato opatření patří k nejdůležitějším z hlediska provozu skladu a jsou též popsána v provozním řádu.
- Celý prostor, ve kterém společnost AZ Elektro provozuje svou činnost, je monitorován kamerovým systémem CCTV.<sup>34</sup> Výjimku tvoří pouze sociální

---

<sup>34</sup> CCTV – Closed Circuit Television – uzavřený televizní okruh.

zařízení a šatny – zaměstnanci, zákazníci i ostatní osoby nacházející se na tomto území jsou s tímto faktem seznámeni.

- Prostor určený k průjezdu nákladních vozidel je hlídán strážní službou, jež vede evidenci vozidel a kontroluje přepravní prostor.
- Strážní na všech stanovištích mají na viditelném místě vyvěšen aktuální bezpečnostní řád.

### 8.3.4 Oblast informačních systémů

- Informační bezpečnost je přijata společností jako ucelený systém vyvážených bezpečnostních opatření doplněných jasně definovaným systémem řízení.
- Bezpečnostním cílem spojeným s využíváním informačního systému (dále IS) je zajištění důvěrnosti a integrity.
- Oddělení IS vytváří vizi IS a prosazuje ji, poznává společnost, zejména z pohledu jeho trhu a zákazníků.
- Oddělení IS pečuje o informační gramotnost pracovníků, dbá na informační vyspělost IS ve společnosti a rozvíjí informační infrastrukturu.
- Oddělení IS připravuje informační strategie, vybírá dodavatele pro nákup IS, s vedením společnosti se podílí na přípravě investic a řízení finančních toků informačních systémů
- Bezpečnostní management eviduje seznam oprávněných uživatelů IS.
- Eviduje též seznam zákazníků internetového obchodu, je správcem osobních údajů a nakládá s nimi dle legislativních požadavků (Úřad pro ochranu osobních údajů).
- Společnost provozuje na stránkách svého obchodu Helpdesk,<sup>35</sup> za nějž je zodpovědné oddělení IS, což je to primární činnost. Služba je provozována nepřetržitě.

---

<sup>35</sup> Helpdesk – v oblasti informačních technologií poskytuje technickou podporu uživatelům PC či jiných zařízení.

- Každý uživatel IS bude jednoznačně identifikován, oddělení IS též vede evidenci všech zařízení.
- Za funkční stránku IS je primárně zodpovědné oddělení informačních systémů, které řeší bezpečnostní otázky s bezpečnostním managementem.
- Každý zaměstnanec, který zaznamená chybu IS, bude ihned kontaktovat oddělení IS.
- Společnost prosazuje zajištění komunikační bezpečnosti způsobem ochrany důvěrnosti a integrity informací během přenosu v LAN<sup>36</sup> sítích.
- Oddělení IS ručí za trvalé dodržování schválené konfigurace hardwaru i softwaru informačního systému včetně nastavení bezpečnostních charakteristik operačního systému a aplikačního softwaru.
- Oddělení IS zkoumá a řeší bezpečnostní incidenty, jež ihned hlásí bezpečnostnímu managementu.
- Oddělení IS ve spolupráci s bezpečnostním managementem zajišťuje školení uživatelů v oblasti bezpečnosti informačního systému.
- Oddělení IS zajišťuje kontrolu bezpečnosti počítačových médií a se závěry seznamuje bezpečnostní management, též se stará o důslednou likvidaci nepotřebných médií.
- Společnost provádí zálohování systémového programového vybavení a zajišťuje ochranu záložních dat.
- Oddělení IS vydává uživatelům výměnná zařízení, přenosné počítače.
- Aktivně zabraňuje neoprávněným otevíráním externích médií přes USB porty.
- Dojde-li k havárii operačního systému, nebo aplikačního SW, oddělení IS zajistí uvedení IS do zabezpečeného stavu dle schválené bezpečnostní dokumentace.

---

<sup>36</sup> LAN – Local Area Network – malá počítačová síť, která pokrývá malé geografické území (například domácnosti, nebo malé firmy)

- Správce sítě jmenovaný oddělením IS, který působí jako správce LAN, musí mít veškeré povinnosti rozšířeny do síťového prostředí. Zde musí být zahrnuta kontrola neporušení kabeláže, aktivních prvků sítě<sup>37</sup>, konfigurace VLAN<sup>38</sup>, apod.
- Oddělení IS má pracovníka kryptografické ochrany, který spravuje kryptografické<sup>39</sup> zabezpečení systémů, kde se pracuje s citlivými daty, jako je například zabezpečení internetového obchodu.
- Oddělení IS sleduje a zabezpečuje pravidelnou aktualizaci antivirových programů a sleduje aktualizaci virových databází.
- Správce sítě spolu s oddělením IS pracují zodpovědně na vyčištění a zotavení systému po napadení virem, po dokončení informují bezpečnostní management.
- Oddělení IS zavádí směrnice pro standardní zahájení práce v IS (identifikace, přihlašovací procedury), pro práci s externími médii (rozhraní USB, DVD, CD), v jakých oblastech na discích může uživatel ukládat data, jaká má uživatel práva.
- Oddělení IS spolupracuje s bezpečnostním managementem nad otázkami přístupu návštěv do IS a k dalším externím pracovníkům (například pracovníci úklidové firmy).
- Bezpečnostní management ve spolupráci s oddělením IS vypracuje krizové plány pro zvládnutí bezpečnostních incidentů a jednotlivě jsou rozpracovány pro určité oblasti (web a internetový obchod, incidenty z pohledu vnitřní bezpečnosti, incidenty poškozující HW a SW).
- Uživatelská hesla jsou na základě osvěty oddělení IS měněna v pravidelných cyklech, oddělení IS informuje uživatele jak správně tvořit hesla.

---

<sup>37</sup> Aktivními prvky sítě jsou zařízení typu: repeater (opakovač), hub (rozbočovač), switch (přepínač), bridge (most), router (směšovač).

<sup>38</sup> VLAN – virtuální LAN – logicky nezávislá síť v rámci jednoho, nebo několika zařízení.

<sup>39</sup> Kryptografie – šifrování.

- Zaměstnanci svá hesla nikde nesdělují ani nezveřejňují, případné incidenty řeší bezpečnostní management, zaměstnanci jsou za tyto prohřešky sankcionováni.

### 8.3.5 Oblast ochrany majetku

- Zaměstnanci společnosti i osoby v externí spolupráci či osoby pohybující se v prostorách nebo nakládající s majetkem společnosti ke své činnosti přistupují zodpovědně a je v jejich zájmu ochrana tohoto majetku.
- Majetek se dělí na movitý a nemovitý, dále na hmotný a nehmotný.
- V případě nemovitého majetku se jedná o administrativní a skladové budovy společnosti, které jsou buď ve vlastnictví společnosti, nebo si společnost pronajímá tyto prostory pro své užívání.
- V případě zjištění závady na tomto majetku je povinností osoby vykonávající zde svou činnost nahlásit příslušný problém správci majetku, který sídlí v kanceláři bezpečnostního managementu.
- Tímto majetkem se též rozumí rozvody inženýrských sítí či další technologické celky, u nichž se zaměstnancům a všem nepovolaným osobám zakazuje manipulace s těmito zařízeními (jedná se zejména o slaboproudá nebo silnoproudá zařízení, rozvody vodní či plynové a jejich zařízení).
- Dále mezi tato zařízení patří zabezpečovací a monitorovací systémy jako je PZS,<sup>40</sup> CCTV.
- Vědomé poškození jakoukoli osobou je považováno za sabotáž a je tudíž řešeno bezpečnostním managementem. Tyto skutky jsou rozděleny do dvou oblastí – vnější narušení a vnitřní narušení.
- Vnější narušením technického zabezpečení společnosti AZ Elektro se rozumí vědomé narušení osobou, která nemá právní vztah vůči společnosti AZ Elektro, tedy není zaměstnancem ani externím spolupracovníkem. Tento skutek bude bezodklad-

---

<sup>40</sup> Poplachové zabezpečovací systémy.

ně oznámen bezpečnostním složkám státu a narušitel bude potrestán dle legislativních norem.

- Vnitřním narušením se rozumí takové narušení, které způsobí vědomě zaměstnanec společnosti, zaměstnanci externích společností nebo osoba evidující se jako návštěva. Tento skutek bude oznámen bezpečnostnímu managementu, který k situaci zaujme stanovisko a poté v závažném případě kontaktuje bezpečnostní složky státu. Bezpečnostní management též diskutuje celou situaci s vedením společnosti a personálním oddělením. Zaměstnanec může být po projednání sankciován, případně s ním bude rozvázána další spolupráce.
- K obsluze těchto zařízení je vyškolen pouze odborný personál, při závadě vždy zasahuje správce majetku, případně bezpečnostní management, který má v případě poruch připraveny havarijní plány pro zvládnutí těchto situací.
- Mezi majetek movitý příkladně řadíme vozový park společnosti, vybavení kanceláře, nábytek, ve skladovacím prostoru regály, manipulační techniku.
- V případě poruchy či dopravní nehody se služebním vozidlem v terénu zaměstnanec vždy kontaktuje asistenční službu, s níž má společnost smlouvu, správce majetku společnosti a policii, jelikož je zde existence třetí osoby a majitelem vozidla je společnost AZ Elektro.
- Každé vozidlo je opatřeno informativní kartou, kde jsou uvedeny všechny důležité kontakty, včetně systému IZS, dále je opatřeno stacionárním sledovacím systémem, který funguje na principu GPS a sleduje aktuální polohu vozidla a spravuje též knihu jízd v elektronické podobě
- Mezi nehmotný majetek patří zejména know-how společnosti a další neveřejné informace jako jsou například finanční výsledky, zprávy, analýzy, audity nebo smlouvy výše uvedené.
- Tento veškerý majetek zaměstnanec musí svým přístupem chránit.
- V případě jakéhokoli pokusu o odcizení zboží jakoukoli osobu v prostorách společnosti (tj. v administrativní budově, skladu, prodejně) je na základě informace ze za-

bezpečovacích systémů osoba zajištěna v souladu s §76 zákona č. 141/1961 Sb.<sup>41</sup> O tomto šetření vždy musí být informována příslušná osoba z řad bezpečnostního managementu, která případ vyhodnotí. Pokud se bude jednat o odcizení majetku zaměstnancem, je s ním vedeno jednání, které může vést k ukončení pracovního poměru, případně náhradě škody a samozřejmě jeho předáním orgánům policie. [18]

- Pro ostatní osoby platí pravidlo již uvedené s tím, že osoba bude po prokázání protiprávního jednání zadržena do příjezdu policie a poté i s důkazy předána.

### 8.3.6 Oblast bezpečnostní a status bezpečnostního managementu

- Bezpečnostní management je správcem bezpečnostní politiky a je přímo zodpovědný za její formu, aplikaci do praxe a dodržování.
- Dále je zodpovědný za její aktualizaci a vypracování jednotlivých provozních řádů pro daná pracoviště.
- Je odpovědný za informovanost všech zaměstnanců o bezpečnostní politice společnosti.
- Je povinen informovat vedení společnosti o mimořádných událostech, respektuje rozhodnutí vedení a je odpovědný za všechna nápravná opatření.
- Má zpracované havarijní plány pro mimořádné situace při nehodách technického charakteru, vždy v několika alternativách.

---

<sup>41</sup> § 76 Zadržení osoby podezřelé – Osobní svobodu osoby, která byla přistižena při trestném činu nebo bezprostředně poté, smí omezit kdokoli, pokud je to nutné ke zjištění její totožnosti, k zamezení útěku nebo k zajištění důkazů. Je však povinen tuto osobu předat ihned policejnímu orgánu; příslušníka ozbrojených sil může též předat nejbližšímu útvaru ozbrojených sil nebo správci posádky. Nelze-li takovou osobu ihned předat, je třeba některému z uvedených orgánů omezení osobní svobody bez odkladu oznámit. [18]

- Má zpracované krizové plány a soubor nápravných opatření pro případ, kdy je narušen stav nehmotných aktiv příkladně vlivem pochybení jedince či útokem z vnějšího prostředí, kterému je povinen předejít a je povinen ho minimalizovat.
- Úzce kooperuje s oddělením informačních systémů a pravidelně analyzuje hrozbu narušení informační bezpečnosti, jak z vnějšího prostředí, tak i z řad vlastních zaměstnanců.
- Nastavuje režimová opatření v prostorech skladu, administrativní budovy a v přilehlém okolí ve vlastnictví společnosti nebo prostor v nájemném vztahu společnosti využívaných.
- Pravidelně kontroluje všechna oddělení, zda dodržují všechna předepsaná pravidla týkající se celkové bezpečnosti.
- Nakládá s firemním majetkem, který spravuje zodpovědně, všechna zásadní rozhodnutí konzultuje s vedením společnosti.
- Management spravuje tzv. provozní knihu, kde jsou zaznamenávány všechny závažné podrobnosti o bezpečnostním systému, jeho činnosti a údržbě.
- Využívá všechny prostředky a komunikační kanály pro dodržování bezpečnostních zásad.
- V případě potřeby komunikuje s bezpečnostními sbory.
- Drží pohotovostní službu nepřetržitě pro případy mimořádných situací, v případě potřeby pověřuje instrukcemi jednotlivé zaměstnance.
- Zpracovává bezpečnostní analýzy a pracuje s výstupy bezpečnostních auditů.
- Bezpečnostní management je zodpovědný za pohyb všech návštěv a zákazníků v zázemí společnosti, tento pohyb se eviduje na základě režimových opatření.
- Provádí správu dokumentace bezpečnosti IS.
- Bezpečnostní management a oddělení informačních systémů spolupracují na systému řízení bezpečnosti informací (ISMS), naplňují všechna jeho kritéria a cíleně pracují na neustálém zlepšování a zkvalitňování tohoto systému.
- Pracuje a stále aktualizuje systém hodnocení rizik a zpracovává mechanismus nápravných opatření.

- Spolupracuje s vedením na jednání ve výrobních závodech, prosazuje systém kontroly jakosti přímo v továrně a připravuje pravidelné kvalitativní audity.
- Vytváří přísné kvalitativní audity a mechanismy, kterými prověřuje dodavatele (subdodavatele či výrobce).
- S oddělením logistiky spolupracuje na postupech reklamace většího objemu zboží, při dodávkách s nalezenými nedostatky na kvalitativní úrovni.

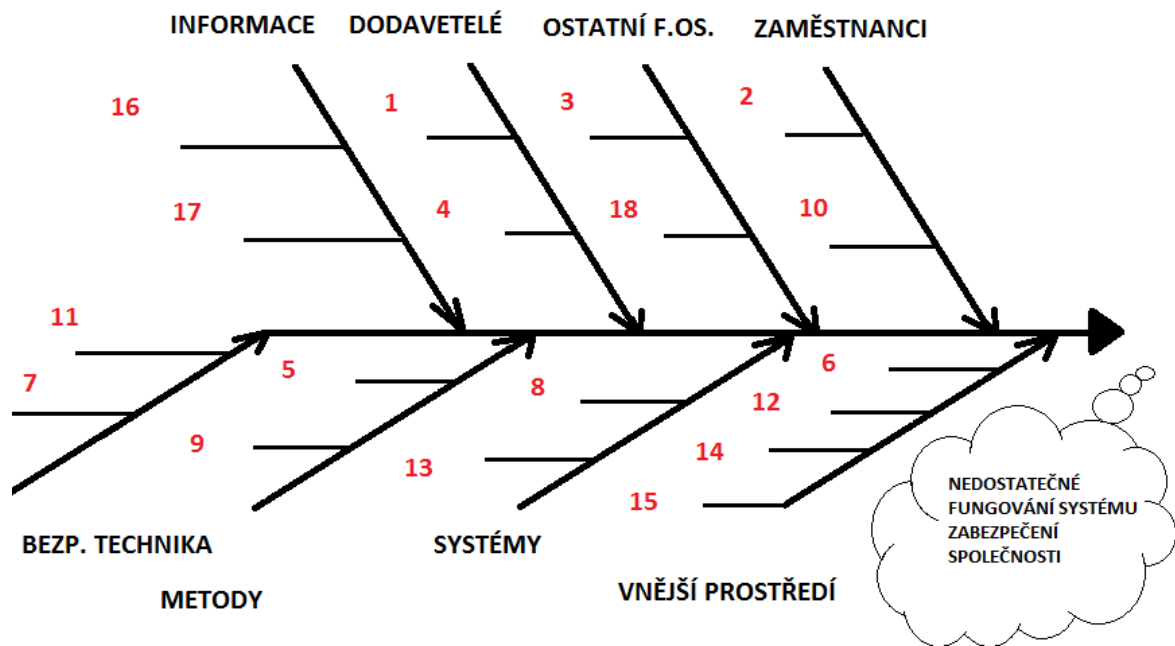
## **9 ZPRACOVÁNÍ BEZPEČNOSTNÍHO PLÁNU ORGANIZACE K ZAVEDENÍ TECHNICKÝCH A TECHNOLOGICKÝCH PROSTŘEDKŮ BEZPEČNOSTI PRO NOVÝ SKLAD SPOLEČNOSTI**

Společnost AZ Elektro se vlivem rostoucích potřeb a zvýšením poptávky ze strany zákazníků internetového obchodu rozhodla pro přesun ze stávajících prostor, které si pronajímá, do nově vybudovaného skladu, jenž pokryje potřeby pro kvalitní logistické zázemí firmy. Celý proces podrobíme systému bezpečnostního plánování se všemi parametry, které jsme si uvedli v předchozích kapitolách. Budeme se snažit o logický postup všech činností za účelem vytvoření bezpečnostního plánu.

### **9.1 ANALÝZA**

#### **9.1.1 Úvaha o přístupu k řešení úkolu**

Stávající systém pro skladování zboží je k poměru prodaného zboží nevyhovující, tudíž je potřeba větší prostor. Ve stávajícím skladě, kde je společnost v nájmu, byly investice do zabezpečení objektu minimální. Pro společnost bylo toto řešení v době jejího vzniku dostačující, časem se objevily určité problémy, týkající se rozkrádání zboží. Sklad společnosti funguje též jako překladiště, avšak větší část zboží zůstává uskladněna. Proto potřebujeme vytvořit prostor, který bude adekvátně zabezpečen proti krádežím. Ty mají několik příčin, jimž je třeba předejít. Velmi důležitá zásada společnosti je rychlé obsloužení zákazníka po jeho objednávce – tj. rychlé vychystání zboží a jeho příprava na doručení k zákazníkovi – způsobem jaký si zákazník určil. Do projektu bude zahrnut bezpečnostní management jako správce projektu, dále nezbytné vedení společnosti, které má všechny rozhodovací pravomoci. Mezi dalšími osobami projektu budou, dodavatelé, projektanti, externí bezpečnostní auditoři a zaměstnanci. Řešíme tedy komplexní expertizu organizace, kde kromě osob, majetku a informací uvnitř firmy chceme chránit osoby, majetek a informace vně organizace. Na základě obecně platných právních předpisů a norem, smluvních závazků a obecně či profesně uznávaných nepsaných pravidel a zvyklostí.

Obr. 16 Analýza současného stavu <sup>42</sup>

### 9.1.2 Benchmarking jako metoda k řízení bezpečnosti v organizaci

V poslední době se často hovoří v souvislosti s řízením organizace o pojmu benchmarking. Z překladu vyplývá, že je to jistý porovnávací bod. Jedna z definic konstatuje, že se jedná o legální, systematický, veřejný, etický a neustále se opakující proces měření, který může výrazně přispět k dosažení konkurenční výhody. Hovoříme o nástroji strategického managementu, jenž systematicky porovnává produkty, procesy nebo metody organizace s jinými relevantními organizacemi. Benchmarking se dá aplikovat na různá odvětví v oblasti managementu, nás však budou zajímat bezpečnostní otázky. Rozlišujeme několik typů benchmarkingu, například:

- **Procesní benchmarking** – porovnáváme výsledky jiných relevantních organizací s cílem identifikovat možná zlepšení vlastních procesů. Podstatou je identifikace správných postupů, poučení se z nich a přizpůsobení jejich prvků podmínkám vlastní organizace, nikoliv pouze okopírování praxe jiné organizace. Větší korporace disponují větší vstřícností v poskytování informací, neboť jsou spolu v interakci subjekty, které si navzájem nekonkurují. Je tedy dobré vybrat takovou organizaci,

<sup>42</sup> Obrázek vlastní

kteřá nebude konkurencí, ale vykonává některé stejné funkce jako naše organizace a to na nejvyšší úrovni.

- **Benchmarking výsledků** – porovnává tvrdá data jako jsou obrat, zisk, produktivita, objem produktů, fluktuace nebo případně spojenost zákazníků. Benchmarking výsledků slouží k tomu, aby organizace zjistila, jakých výsledků dosahuje v porovnání s konkurencí. Získaná data jsou následně využitelná při plánování strategií i stanovování vlastních cílových hodnot. [44]

Dále dělíme metody benchmarkingu na:

- **Interní** – obchodní jednotky v rámci organizace
- **Externí** – porovnání mezi organizacemi)

Cílem tedy bude vytvořit komplexní systém řízení bezpečnosti, který se bude dotýkat těchto oblastí:

- Oblast řízení
  - Řízení společnosti a jejích závazků
  - Systém řízení a komunikace
  - Hodnocení, audity a měření
- Provozní oblast
  - Identifikace s minimalizace rizik
  - Pracovní prostor
  - Provozní procesy a postupy
- Oblast personální
  - Zapojení pracovníků a vedení
  - Motivace, chování, postoje
  - Školení a velmi důležité ankety zaměstnanců pomocí dotazníků [47]

#### **9.1.2.1 Výhody benchmarkingu**

- předchází objevování již objeveného,
- napomáhá implementaci nových, neotřelých postupů v organizaci,

- motivuje organizace k prověřování vlastních procesů,
- napomáhá překonávat skepsi a nedůvěru vůči novým postupům (zamýšlená změna se již osvědčila),
- napomáhá k sestavení realistických cílů. [40]

Benchmarking je také zakotven v našich normativních předpisech – ČSN EN ISO 9004:2010 [28]

### 9.1.3 Sběr informací

Dle Işikavova diagramu, který je variantou analýzy příčin a následků (CCA) rozdělíme informace do několika kategorií pro větší přehled a v nich utvoříme pořadí dle našich priorit.

- **Kategorie zaměstnanci**
  - Zvažujeme princip, jakým jsou zaměstnanci vybírání pro své pozice.
  - Cítí se zaměstnanci spokojeně ve společnosti?
  - Jak se lišíme s rámci spokojenosti zaměstnanců od konkurence?
  - Jaký je zaveden pro zaměstnance sociální program?
  - Jsou zaměstnanci dobře motivováni a finančně odměňováni?
  - Jaká je míra fluktuace?
  - Co zaměstnance vede k odcizení zboží?
  - Jak přistupovat k zaměstnanci, který odcizí zboží ve společnosti?
  - Nutnost školení zaměstnanců
  - Kvalita a úroveň komunikace mezi zaměstnanci
  - Práva a povinnosti zaměstnance
- **Kategorie zabezpečovací technika**
  - Požadavky na zabezpečovací techniku
  - Pořizovací cena
  - Vhodnost nasazení zabezpečovací techniky
  - Sledování aktuálních trendů v zabezpečovací technice

- Úroveň servisů, revizí a pozáručního servisu
- **Kategorie ostatní fyzické osoby**
  - Kontrola pohybu cizích osob po objektu
  - Informovanost a kontrola brigádníků najatých personální agenturou, se kterou spolupracujeme
  - Zpětná vazba mezi společností a personální agenturou
- **Kategorie dodavatelů a služeb souvisejících s bezpečností organizace**
  - Počet a prověření dodavatelů
  - Bezpečnostní úroveň dodavatelských společností
  - Ekonomická stabilita dodavatelských organizací
  - Závislost na dodavatelích bezpečnostních služeb a techniky
  - Poměr kvality a ceny
- **Kategorie metody**
  - Stav kontrolních mechanismů společnosti
  - Vytvoření a prosazování bezpečnostní politiky
  - Kvalita signalizace hrozeb
  - Řídící schopnosti vedoucích pracovníků
  - Schopnosti bezpečnostního managementu
  - Zvládání rizik
  - Předcházení krizovým situacím
- **Kategorie informace**
  - Informační systém společnosti a jeho použití
  - Úroveň bezpečnosti informačního systému ve společnosti
  - Zabezpečení provozu internetového obchodu
  - Skladový systém
  - Citlivé informace uvnitř organizace

- Politika informační bezpečnosti
- Řízení rizik
- **Kategorie systémy**
  - Vhodnost použitých systému zabezpečení
  - Rozpočet pro nasazení bezpečnostní techniky
  - Zpracování provozních řádů
- **Kategorie vnější prostředí**
  - Legislativa (zákoník práce, ochrana osobních údajů, občanský zákoník)
  - Tuzemské a mezinárodní standardy
  - Potřeby zákazníků
  - Vliv konkurence

#### 9.1.4 Třídění a výběr informací

Uvedli jsme si jednotlivé body, které pro nás budou důležité a rozdělené do jednotlivých kategorií. Každému z nich tedy přidělíme příslušnou váhu a pokusíme se řadit naše priority v určitém pořadí. Jako obchodní společnost uvažujeme tedy o existenci a o předmětu podnikání. Zisk naší společností tvoří zákazníci, proto by celý systém měl být orientovaný směrem k potřebám zákazníka. Uvědomujeme si však, že tato cesta je velmi složitá a bez týmu kvalitních zaměstnanců toho společnost nedosáhne. Ve společnosti v současné době je zaměstnáno 200 lidí. Není v našich možnostech osobně poznat všechny zaměstnance a jednotlivě znát jejich potřeby a zájmy. Důležité je tedy motivovat zaměstnance k dosažení výkonu. Zaměstnanec je přijat na základě určité procedury přijímacího řízení, které má na starost personální oddělení – tam jsme schopni vytipovat určité vlastnosti a znalosti zaměstnance, které by mohl v naší společnosti uplatnit. Avšak není v našich schopnostech poznat každého zaměstnance dokonale a určit jeho hodnoty. Dalším velmi důležitým parametrem bude zabezpečení, to bude mít i preventivní charakter jak ze strany vnitřních vztahů, tak bude mít vliv i na vnější prostředí. Potřebujeme tedy zajistit systém, který bude pracovat na kvalitní informační infrastruktuře, bude mít adekvátní bezpečnostní prvky a zároveň bude efektivní a nebude těžkopádný. Zaměříme se tedy na oblasti, kde dochází ke ztrátám a pro další konání bude cílem zvýšení bezpečnostních požadavků tak, aby tento systém neměl negativní vliv na koncového zákazníka.

Informace relevantní pro bezpečnostní analýzu uvnitř společnosti:

- V základních ustavujících dokumentech v předmětu činnosti
- V organizačních a interních předpisech společnosti, včetně její organizační struktury
- Technické a technologické vybavení
- V architektonickém a stavebním řešení objektu, ve kterých organizace působí
- V definovaných vztazích nadřízenosti a podřízenosti mezi jednotlivými pracovníky
- Určení osobních odpovědností zaměstnanců v rámci jejich působení ve firmě
- V personálním složení organizace a zásadách personální politiky
- V rozsahu a struktuře dodavatelsko-odběratelských vztahů
- V obchodní politice organizace a jejích vytyčených cílech
- Ve vnitřní situaci organizace a jejím trendu

Informace relevantní pro bezpečnostní analýzu vně společnosti:

- V mezinárodních smlouvách a závazcích
- V mezinárodních standardech a doporučeních
- V tuzemských právních předpisech, standardech a doporučeních
- V celospolečenské situaci a jejím trendu

Uvedené informace mají zpravidla ustálenou formalizovanou podobu:

- Originální písemnosti a dokumenty
- Články a studie
- Statistické výkazy
- Ústní a písemná vyjádření, komentáře fyzických osob (zpravidla vedení společnosti a zaměstnanců k analyzovanému problému)
- Dotazníkový průzkum vybraných pracovníků
- Vlastní pozorování pracovníků, kteří sběr provádějí
- Informace získané z internetu atd.

### 9.1.5 Studium a rozbor

Po zpracování všech událostí, které vedou ke ztrátám společnosti jsme zjistili, že se tyto úniky dají kategorizovat do několika skupin. Grafické znázornění nám pomůže najít jednotlivé nedostatky.

- 1. Ztráty zboží během přepravy
- 2. Rozkrádání zboží zaměstnanci, nefunkčnost bezpečnostního dohledu z řad vlastních zaměstnanců
- 3. Rozkrádání zboží externími zaměstnanci (brigádníci, řidiči)
- 4. Úmyslné či neúmyslné chyby v dodávkách zboží od dodavatelů
- 5. Chyby při inventarizaci zboží
- 6. Škody na majetku vlivem vandalství osob z vnějšího prostředí
- 7. Útoky hackerů na servery provozující internetový obchod
- 8. Přílišná tolerantnost a absence bezpečnostní politiky
- 9. Neefektivní řízení a plánování směn a tím vznikající nadměrné zatížení, narůstající chaos či naopak nedostatek práce pro zaměstnance
- 10. Nedostatečná komunikace mezi jednotlivými pracovními skupinami
- 11. Zastaralost zabezpečovacích systémů
- 12. Nedostatky z pohledu zákoníku práce
- 13. Nedodržování BOZP
- 14. Prodlužování dodacích lhůt, nespokojenost zákazníků
- 15. Nerovnoměrný konkurenční boj
- 16. Pohyb citlivých informací po společnosti
- 17. Zastaralý a nefunkční informační systém, včetně skladového systému
- 18. Pohyb návštěv v prostorách společnosti
- 19. Nejednoznačné kompetence v jednotlivých odděleních

### 9.1.5.1 *Metody sběru dat:*

- Rozhovor se zástupci vedení organizace
- Dotazníky
- Pozorování
- Analýzy dokumentů

Úskalí a nepříznivé faktory v budoucím procesu plánování:

- Problém přebírání vzorů (to, co pomůže jiné organizaci nemusí pomoci nám)
- Nutnost rozsáhlého získávání informací, příprava pracovníků na realizaci benchmarkingu a implementace změn
- V procesu benchmarkingu – každá organizace není ochotna sdílet důležité informace o svém procesu
- Neochota zaměstnanců ke změně
- Slabá komunikace, či nedostatečné schopnosti zaměstnanců
- Nedostatečné porozumění procesům změn vedoucím k lepšímu systému zabezpečení
- Slabé plánování, nebo použití nevhodné metody

Informace třídíme dle časového významu, podle vlivu na řešení analýzy, podle dostupnosti na veřejné a neveřejné, podle věrohodnosti, podle oblasti, které se dotýkají.

### 9.1.6 **Zobecnění**

Musíme tedy určit pravidla v klíčových oblastech, těmi budou bezpečnostní technika, zaměstnanci, vnější prostředí, informace, systémy. Tyto otázky budou pro nás klíčové a z nich budeme vycházet v bezpečnostním plánování. Oblasti jsou setříděny dle priorit a bude důležité nalézt vazby mezi těmito oblastmi.

## 9.2 **ROZHODOVÁNÍ**

### 9.2.1 **Ujasnění problému**

Společnost tedy stojí před rozhodnutím, jakým směrem v oblasti bezpečnosti se chce prosadit. Podporou vedení v těchto otázkách bude bezpečnostní management, který určí směry

a navrhne varianty řešení. Bude se jednat o komplexní řešení bezpečnosti pro objekt skladu a na něj navazující bezpečnostní opatření. Jinými slovy o dobře zpracovanou bezpečnostní politiku; vytvoření mechanismu, který bude tato opatření prosazovat a případně trestat jejich narušování či nedodržování. Dále bude důležité zvolit vhodné nasazení bezpečnostních systémů, které bude účinné a bude adekvátní ekonomickým možnostem společnosti.

## 9.2.2 Zpracování variant postupu řízení

### 9.2.2.1 Varianta 1

Tato varianta připouští měkčí pravidla z pohledu zabezpečení a v podstatě kopíruje stávající situaci. Do prostor objektu je nainstalován kamerový systém CCTV, spolu s elektronickou požární signalizací a poplachovými zabezpečovacími systémy. Fyzickou bezpečnost zajišťují kmenoví zaměstnanci společnosti. Jelikož je zde společnost v nájmu, nájemce tolik neinvestuje do systému zabezpečení a například opomíjí otázky plášťové ochrany. Z tohoto důvodu se v minulosti stávalo, že se osoba z vnějšího prostředí snažila dostat přes okenní výplně do prostoru skladu. Zabezpečení je na nízké úrovni, avšak z pohledu ekonomické náročnosti není nákladné, protože společnost měla nájemní smlouvu na dobu určitou a neměla důvod příliš investovat do zabezpečení z vlastních zdrojů. Tato varianta je přípustná jako přechodné řešení dokud společnost nenajde lepší prostory.

### 9.2.2.2 Varianta 2

V místě logistické zóny, kde má společnost zájem vybudovat sklad, se nachází logistická firma zabývající se přepravou trvanlivých potravin. Společnost si zjišťuje stav zabezpečení těchto prostor, aby případně získala zkušenosti z praxe jiné firmy. Na rozdíl od naší společnosti je bezpečnost zajišťována dodavatelským způsobem bezpečnostní agenturou. Společnost zde spatřuje i kladné body v úspoře nákladů, administrativy a odvodů z mezd stálých zaměstnanců. Pozoruje vzájemné vazby mezi zaměstnanci, které mohou ve výsledku firmu poškozovat. Bezpečnostní agentura v okolí provozuje bezpečnostní činnost v několika objektech a může si dovolit pravidelně zaměstnance střídat mezi objekty, aby nedocházelo k těmto nepříznivým vazbám. Je zde však patrný rozdíl mezi těmito společnostmi, kde jsou nastavena bezpečnostní pravidla, ale společnost si není jistá, zda by byly pro její potřebu dostačující. Ve výsledku bude tedy tato varianta nákladnější, než první, je to však investice do bezpečnosti. Otázkou zůstává, zda převzetí vzoru bude plně v souladu s požadavky organizace.

### 9.2.2.3 *Varianta 3*

V této variantě vychází společnost z předpokladu, že si najme pro zajištění fyzické bezpečnosti služby bezpečnostní agentury. Svou pozornost zaměří na zabezpečení skladovacích prostor, kde se na malém místě nachází poměrně mnoho zboží menších rozměrů, avšak v hodnotě stovek tisíc korun. Zjišťují se možnosti dokonalejšího zabezpečení kamerovými systémy, zajištění prvků předmětové ochrany v kombinaci s mechanickými zábrannými systémy. Tato investice je poměrně nákladná. Je ale nutno vedení sdělit hodnotu aktuálních ztrát, které by těmito opatřeními mohly být minimalizovány. Dále je také vhodné podotknout, že společnost hodlá zvýšit svůj obrat, tudíž riziko ztrát by se mohlo ještě zvětšit. Je třeba k situaci přistupovat systémově, kdy máme za cíl dosáhnout určitého bezpečnostního stupně za předpokladu nutných investic. Existuje možnost nastavit určité podmínky a systémy na zkušební období a poté zvážit další kroky.

### 9.2.2.4 *Varianta 4*

Tato varianta počítá s investicí větších rozměrů, avšak z pohledu systému je komplexní, ucelenou a funkční s minimalizací dalších investic. Opět vycházíme z pohledu fyzické bezpečnosti na dodavatelské službě bezpečnostní agentury, výběr této organizace bude zapotřebí dobře zvážit. Zde tedy zkusíme postihnout všechny části bezpečnostního systému, abychom utvořili fungující systém ve všech směrech a nevázáli se pouze na otázku nákladů. Budeme tedy řešit jednotlivé body jak fyzické, tak i technické bezpečnosti. V technické části budou rozvedeny otázky prostorové, předmětové i plášťové ochrany. Samozřejmostí je otázka poplachových systémů a všech prvků, které je nutné splnit v rámci naší legislativy při stavebních úpravách. Bude instalován přístupový systém, který nám zabezpečí kontrolu vstupu a výstupu ze skladu. Nástavbou bude nový docházkový systém, který zjednoduší práci personálnímu oddělení a zajistí nám kontrolu pohybu zaměstnanců. Tato varianta bude nejnákladnější, existuje však úvaha, že z dlouhodobého hlediska vyřeší naše bezpečnostní problémy a vytvoří pevný systém.

## 9.2.3 **Volba optimální varianty a formulace rozhodnutí**

Společnost se rozhodla zvolit variantu číslo 4. Tato varianta vyhrála pro její komplexní pohled. Bude se sice jednat o nákladnou investici, ale firma zde sledává mnoho pozitivních parametrů. Pomůže jí naplnit již sestavenou bezpečnostní politiku. S bezpečnostním

managementem bude nyní rozebrána celá řada úkolů, které bude třeba v bezpečnostním plánování vyřešit.

## 9.3 PLÁNOVÁNÍ

### 9.3.1 Určení omezujících podmínek

Mezi základní parametry bude patřit

- míra bezpečnosti
- doba realizace
- finanční zajištění
- odpovědnost
- bezpečnostní posouzení objektu
- odborná způsobilost a dobré reference dodavatelských společností

### 9.3.2 Formulace základních předpovědí

Vedení společnosti s bezpečnostním managementem nejprve zpracuje zadání projektu, kde budou jasně vyznačeny základní požadavky na systém. Poté bude následovat jednání s možnými dodavateli a probíhá tedy konzultační činnost na několika úrovních s cílem vybrat vhodného dodavatele služeb. Společnost si nechá zpracovat od dodavatelských společností studie, v nichž budou představeny různé přístupy k řešení problematiky zabezpečení skladových prostor. Cílem této činnosti bude výběr vhodného dodavatele, jenž bude splňovat nejvíce parametrů. Následuje zpracování projektové dokumentace, koordinace činností, dozorová činnost, dále vlastní instalace technologií. Po dokončení instalace proběhnou funkční zkoušky, řízení projektu, jednání s dodavatelem o servisních prohlídkách, záruce a nakonec předání díla. V neposlední řadě koordinace s HZS kraje na zpracování krizových plánů a revizích EPS. Poté bude nastavena doba zkoušek systému, na jejímž konci bude zhodnocen stav a případně bude korigován další postup.

#### 9.3.2.1 *Bezpečnostní posouzení objektu*

Ve střežených objektech existuje řada faktorů, které mohou ovlivnit správnou funkci PZTS a vyvolávat plané poplarchy. Těmto faktorům je třeba předcházet a podle nich zvažovat

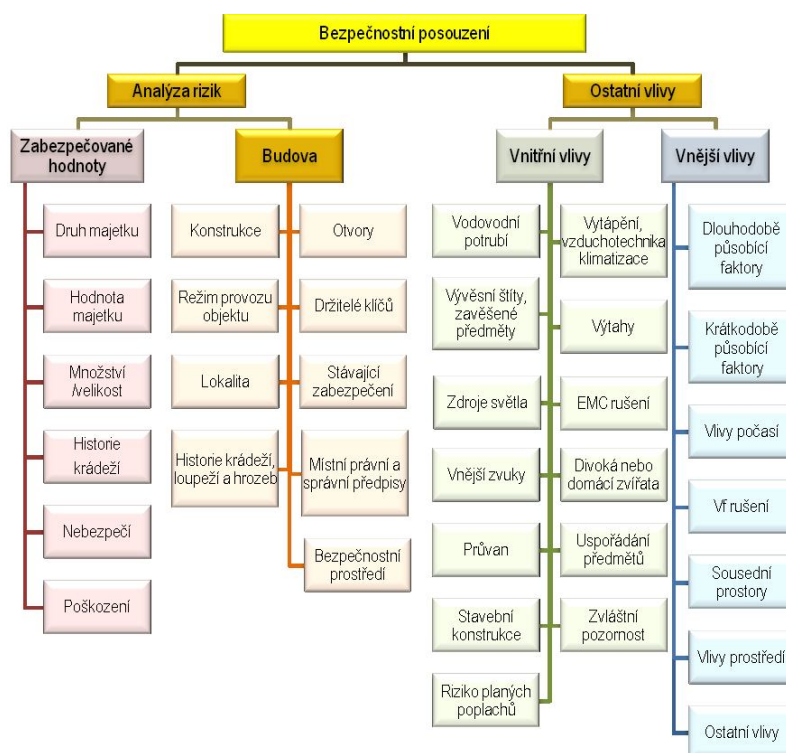
umístění a druh zabezpečení. Je třeba tyto faktory podrobit analýze a vyhodnotit správné nasazení pro PZTS. Nejpravděpodobnější **vnitřní vlivy** působící plané poplachy jsou:

- **Vodovodní potrubí** – proudění vody v plastovém potrubí a vliv na funkci mikrovlnných detektorů.
- **Vytápění a vzduchotechnika** – turbulentní vzduch vznikající činností vzduchotechniky.
- **Výtahy** – ovlivnění funkce detektorů vibracemi.
- **Zdroje světla** – fluorescenční světelné zdroje mohou nepříznivě ovlivňovat činnost mikrovlnných detektorů. Kompaktní výbojky, které jsou zdrojem vysoké hladiny elektromagnetického rušení a bodové reflektory, jež jsou nasměrovány na čočky či zrcadla pasivního infračerveného detektoru také mohou způsobit řadu planých poplachů.
- **Elektromagnetické rušení** – může jej představovat veškeré vybavení objektu negativně ovlivňující zařízení PZTS. Konkrétně se jedná o napájecí nebo signální vedení.
- **Vnější zvuky** – pokud jsou v objektu používány ultrazvukové detektory. Nejčastěji to bývají zvuky způsobené telefonními zvonky, kompresory či netěsnostmi ve vzduchových potrubích.
- **Průvan** – negativně ovlivňuje funkci ultrazvukových a infračervených detektorů.
- **Uspořádání skladovaných předmětů** – zde je nutné dodržovat a pravidelně kontrolovat způsob skladování na té úrovni, aby zboží nezasahovalo do zóny, kterou detektor zabezpečuje.
- **Stavební konstrukce střežených objektů** – zde sledujeme například konstrukci střech. Je zde nutná specifická konfigurace detektorů pro daný případ.

Vnější vlivy působící na PZTS, jsou takové, které směřují k objektu z vnějšku a nemůžeme je ovlivnit. Musíme proto tyto vlivy specifikovat a pokusit se minimalizovat jejich dopad na náš systém:

- **Dlouhodobě působící faktory** – například silnice, železnice, včetně podzemních dopravních systémů či letecké dopravy, dále například parkoviště nebo přírodní vlivy.

- **Krátkodobě působící faktory** – sem patří zejména vlivy působení staveb v přilehlém okolí.
- **Vlivy počasí** – například působení silných povětrnostních podmínek, působení blesků.
- **Vysokofrekvenční rušení** – ta způsobují vysílače veřejné sítě, televize, antény civilních, vojenských radarů, základnové stanice systému GSM, atp.
- **Sousední objekty** – zejména používání těžkých stojů (vibrace) nebo vysoká hladina elektromagnetického rušení svářecí technikou.
- **Vlivy klimatických podmínek** – zařízení musí splňovat parametry jako je rozsah teplot či míra vlhkosti.
- **Ostatní vlivy** – pohyb osob nebo divoké zvěře v okolí perimetru střeženého objektu. [14]

Obr. 17 Bezpečnostní posouzení<sup>43</sup>

<sup>43</sup> Převzato z: VALOUCH, Jan. *Projektování bezpečnostních systémů*. 1. vyd. Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-230-5.

### 9.3.3 Stanovení konkrétních úkolů

- Zajistit osobní, informační a majetkovou bezpečnost za použití mechanické ochrany, elektronické a režimové ochrany.
- Zajistit kooperaci a součinnost všech subjektů zařazených do projektu.
- V každém bodu plánu je uvedena osoba, která za danou situaci zodpovídá. Pokud má tuto odpovědnost více z nich, uvede se adresně kdo a za co odpovídá
- Vyhovět všem normám a legislativním požadavkům.
- Minimalizovat rizika hrozeb.
- Dodržet daný rozpočet.
- Zpracovat krizové plány.

### 9.3.4 Určení prostředků činnosti

Vypracování bezpečnostní dokumentace bezpečnostní ochrany objektu:

- **Pravidla pro výkon strážné služby**
- **Plán ochrany objektu**
  - Režimová opatření
  - Fyzická ochrana
  - Technická ochrana
    - CCTV systémy
    - Poplachové zabezpečovací systémy
    - Požární bezpečnost
    - Systémy kontroly vstupů
    - Spojení na dohledová a poplachová přijímací centra
- **Provozní řád objektu**
- **Plán krizové připravenosti**

### 9.3.5 Vypracování plánu postupu řízení

Vše by mělo být zpracované v písemné a grafické formě, výsledek plánování po grafické stránce je uveden v přílohách.

## 9.4 Plán ochrany objektu

### 9.4.1 Režimová opatření

Představují procesní naplnění bezpečnostní politiky organizace

#### 9.4.1.1 *Kontrola vstupu do objektu skladu*

- Zaměstnanci – jsou vybaveni čipovou kartou, s níž procházejí vstupním turniketem do skladu.
- Návštěvy – jsou povinně zaregistrovány v prostoru vstupu a do skladu smějí pouze s doprovodem strážného, nebo pracovníka společnosti.
- Do registračních údajů patří, jméno a účel návštěvy či jméno zaměstnance, za nímž návštěva přichází.
- Za turniketem se nachází bezpečnostní rám, který reaguje na bezpečnostní štítky, kterými jsou skrytě zabezpečeny předměty menší velikosti.
- Každý, kdo opouští sklad, je podroben fyzické kontrole a na vyžádání strážného poskytne k nahlédnutí svá zavazadla.
- Strážný je odpovědný za evidenci návštěv, při mimořádné události zavolá velitele objektu ve směně a sepíše s osobou záznam o události, kde bude popsána situace a od obou stran podepsána.
- Každá osoba vstupující do prostoru skladu je vybavena viditelnou reflexní vestou.

#### 9.4.1.2 *Pohyb v prostorách skladu*

- Zaměstnanci mají povolen vstup na místa podle svého zařazení, všechny dveřní systémy mezi pracovištěm v budově jsou vybaveny čtečkami karet, které jsou přednastaveny pro dané zaměstnance, takže je zamezen nepovolený přístup do prostor, kde zaměstnanec nevykonává svou činnost.

- Návštěvy jsou vybavené viditelnou kartou „NÁVŠTĚVA/VISITOR“, pro její pohyb platí výše uvedené.
- Pohyb osob ve skladu je omezen na prostor vyznačený na podlaze; z této trasy nesmí procházející osoba odbočit, hrozí totiž riziko střetu s manipulační technikou.

#### 9.4.1.3 Pravidla pro řidiče externích společností

- Každý řidič se před vjezdem do objektu zaregistruje na vrátnici, kde zaznamenají jeho jméno, SPZ, společnost pro kterou pracuje.
- Prostor vrátnice je opatřen bezpečnostními závorami.
- Podmínkou pro vjezd je použití reflexní vesty a plné obuvi.
- Následně bude strážným nafocen ložný prostor.
- Založí řidiči **doklad o pohybu zboží**, který řidič podepíše s tím, že souhlasí s kontrolou; pokud řidič tento doklad nepodepíše, nebude do objektu vpuštěn. Při odjezdu doklad odevzdá a strážný opět vyfotí ložný prostor a zkontroluje údaje na dokladu.
- Doklad je rozdělen do dvou částí – část přepravního prostoru a část kabiny řidiče.
- Součástí dokladu je počet přivážených palet, z toho EURO palet, příp. balíků, přepravek, dále všechny předměty – jako jsou paletové vozíky atp. v ložném prostoru. Počet palet nebo balíků, které nejsou určeny pro tento sklad. Vyplní též stručný seznam předmětů nacházejících se v kabině řidiče.
- Při výjezdu strážný zkontroluje přepravní prostor vozidla, vyplněné doklady od zaměstnanců společnosti, kde je zaznamenáno, kolik palet bylo vyloženo, nebo naloženo. Dále při výjezdu vozidla zkontroluje prostor kabiny řidiče, porovná se vstupními údaji a poté povolí odjezd řidiči.
- V případě, že strážný zjistí rozdílné počty v dokladech a zboží, které řidič veze, kontaktuje pracovníky skladu, kde žádá nápravu; v opačném případě je na místo přivolán velitel objektu ve směně a je sepsán záznam o události.



Obr. 18 Kontrola vjezdu do objektu <sup>44</sup>

#### 9.4.1.4 *Kontrola příjmu zboží*

- Každá dodávka zboží je zkontrolována dle kvantitativního a kvalitativního hlediska zaměstnancem příjmu zboží, který pomocí čtecího zařízení načte kódy ze zboží s počty kusů do systému a ten vyhodnotí, zda je objednávka v pořádku.
- Za tuto činnost primárně odpovídá zaměstnanec.
- Zaměstnanec strážné služby na úseku příjmu zboží kontroluje náhodně stav objednávek, zda bylo přijato vše v pořádku. Až poté zboží označí a může být dále se zbožím manipulováno.

---

<sup>44</sup> Převezato z: *ICVV: Realizace projektu* [online]. 2012 [cit. 2014-05-20]. Dostupné z: <http://www.icvv.cz/realizace>

- Zaměstnanec strážné služby musí splnit denní limit kontroly všech objednávek, který stanoví minimum 80% zkontrolovaného zboží.

#### **9.4.1.5 Kontrola výdeje zboží**

- Veškeré zboží, které odchází ze skladu, zaměstnanec výdeje zboží zkontroluje pomocí čtečky, kde načte čárový kód a systém mu ukáže počet kusů a místo dodání, zaměstnanec tyto údaje kontroluje.
- Za tuto činnost primárně odpovídá zaměstnanec.
- Zaměstnanec strážné služby kontroluje správnost údajů, zboží po kontrole označí a může být tedy naloženo.
- Denní limit strážného pro kontrolu výdeje je 80% zkontrolovaných z celkového počtu objednávek k výdeji.

#### **9.4.1.6 Speciální režimová oprávnění skladu**

- Velitel objektu ve směně má pravomoc, provést na příkaz bezpečnostního managementu zkoušku na alkohol či jiné návykové látky každému zaměstnanci společnosti. V případě, že se zaměstnanec nebude chtít podrobit, bude s ním nakládáno jako by zkouška dopadla pozitivně. Pokud se zaměstnanci prokáže pozitivní test, jedná se o hrubě porušení pracovní kázně, jež bude řešeno v personálním oddělení.
- U manipulace se zbožím v oddělení A bude vždy přítomen zaměstnanec bezpečnostní služby a provede záznam o kontrole. Zde je zpřísněn režim vzhledem k tomu, že je zde uskladněno zboží jako PC, notebooky, mobilní telefony, flash disky, telefonní karty, fotoaparáty, kamery, navigace, externí disky a komponenty na PC a další drobná elektronika.
- Po ukončení pracovní doby skladu, velitel zastřeží všechny bezpečnostní systémy a v prostoru se nesmí pohybovat žádná osoba, pouze strážný, který zde vykonává pochůzky a pomocí mobilní aplikace obchází kontrolní trasu.
- Velitel objektu ve směně má na starosti manipulaci s klíči, kódy elektrické zabezpečovací signalizace a ovládání identifikačních prvků systému kontroly vstupu v součinnosti s personálním oddělením.

### 9.4.2 Fyzická ochrana

Fyzickou kontrolu provádí bezpečnostní agentura, která byla předem prověřena a splňovala požadavky a kritéria na náplň své činnosti, z pohledu managementu. Je pravidelně kontrolována a sleduje se její činnost. V pravidelných cyklech se schází zástupci bezpečnostní agentury s bezpečnostním managementem organizace na poradách, kde hodnotí stav situace, mimořádné události a další kritéria kontrolní činnosti bezpečnostního managementu.

#### 9.4.2.1 Pravidla pro výkon strážní služby

- Výkon služby je rozdělen do dvou směn – denní 6.00 – 18.00, noční 18.00 – 6.00.
- Každý strážný je povinen po příchodu do zaměstnání či převzetí služby zapsat záznam do knihy služeb.
- Při předání služby je nutné předání všech informací k zabezpečení řádného chodu strážní služby v místě svého výkonu.
- Předmět ochrany je zamezení vstupu cizích osob do objektu, zamezení vynesení jakýchkoliv předmětů a informací bez vědomí společnosti, preventivní ochrana před mimořádnými nebo havarijními událostmi, případně spolupráce na jejich zvládnutí.
- Strážný dodržuje stanovený režim, který je určen pro jeho vykonávání (například provádění nepravidelných pochůzek k zajištění bezpečnosti perimetru objektu).
- V pracovní době klade hlavní důraz na kontrolní činnost.
- Zajišťuje evidenci pohybu ohlášených i neohlášených osob a vozidel, které dále zapisuje do knihy návštěv, nebo knihy vjezdů a výjezdů.
- Při zjištění protiprávní činnosti informuje vedoucího objektu a vykoná zápis do knihy mimořádných událostí.
- Je oprávněna použít v zájmu ochrany života, zdraví zaměstnanců a majetku společnosti přiměřeným způsobem věcné bezpečnostní prostředky a každá tato událost musí být zaznamenána v knize mimořádných událostí.
- Pokud byly použity věcné bezpečnostní prostředky, musí být učiněn záznam v knize zásahů.

- Vedení soukromé bezpečnostní služby plně spolupracuje s bezpečnostním managementem společnosti, s nímž se podílí na řídicích organizačních a kontrolních úkonech.
- Bezpečnostní management kontroluje zápisy z provozních knih, aby splňovaly dané požadavky a byly informačně přesné.
- SBS na konci měsíce provádí měsíční uzávěrku a podílí se s bezpečnostním managementem na personální práci a kontrolní činnosti.
- Zaměstnanec strážní služby je povinen nastupovat do služby včas dle rozpisu, náležitě upravený a ve služebním stejnokroji a v takovém stavu, aby jeho činnost v žádném případě nebyla ovlivněna návykovými látkami (alkohol, léky či jiné látky).
- Zaměstnanec strážní služby nesmí ukončit směnu dříve, než bude předána směna, musí dodržovat vnitřní předpisy společnosti, chránit majetek společnosti před zničením, poškozením, nebo odcizením, dále musí znát předpisy a postupy související s narušením objektu nepovolanou osobou.
- Zaměstnanec bezpečnostní služby musí ovládat obsluhu hlavních uzávěrů vody, plynu, elektřiny a technologických zařízení.
- Musí ovládat rozmístění a ovládání zabezpečovacích systémů a rozeznat pravidelný režim od poruchy, neodkladně odstraňovat zjištěné nedostatky, které by mohly vést ke vzniku požáru a pokud to nebude v jeho silách, je povinen vše oznámit svému nadřízenému.
- Kontroluje uzamčení střežených prostor.
- Kontroluje ložné plochy vozidel pohybujících se ve společnosti a vyžaduje vysvětlení.
- Zamezuje výjezdu vozidlům při podezření na nelegální vývoz zboží.
- Zaměstnanec má právo vyzvat každého, kdo ohrožuje zdraví nebo život jiné osoby, nebo poškozuje majetek a porušuje pravidla občanského soužití, aby od takového jednání upustil.

- Zaměstnanec má právo zadržet osobu, která byla přistižena při trestném činu nebo bezprostředně po něm. Zadržuje ji pro zjištění její totožnosti nebo cílem zabránit útěku do příjezdu policie, jíž musí osobu ihned předat.
- Pracovníkům strážní služby je zakázáno požívat alkoholické nápoje, nebo jiné látky snižující způsobilost pro výkon služby, svévolně měnit rozpis směn bez vědomí nadřízených, nebezpečně nebo neopatrně zacházet s věcnými bezpečnostními prostředky, opouštět stanoviště mimo služební účely, přijímat na stanovišti soukromé návštěvy, poskytovat informace nepovolaným osobám.
- Kontrolu pracovníků soukromé bezpečnostní služby může vykonávat vedení společnosti, nebo bezpečnostní management a vykoná zápis do knihy služeb.

Výzbroj a výstroj: Služební stejnokroj (košile s označením, kravata, černé kalhoty, pevná obuv nebo černý maskovací oděv, černé triko a kanady, opasek), slzný plyn, pouta, tonfa, svítilna, doklady (služební průkaz, průkaz odborné způsobilosti).

Seznam evidence na stanovištích strážní služby: směrnice pro výkon služby, kniha služeb, kniha mimořádných událostí, kniha zásahů, inspekční kniha, kniha návštěv, kniha evidence vozidel, kniha evidence a výdeje klíčů, kniha propustek, požární kniha. [46]

#### 9.4.2.2 Harmonogram fyzické ochrany objektu

Druh činnosti	DEN	NOC
Velitel objektu ve směně	1	1
Zástupce velitele	1	0
Strážný personálního vstupu a recepce	2	1
Kontrola příjmu zboží	1	0
Kontrola výdeje zboží	1	0
Strážný ve vrátnici	2	1
Strážný oddělení A	2	1
Strážný oddělení B a C	1	0
Venkovní ostraha objektu	1	1
Střídač	1	0
<b>Celkem zaměstnanců na směnu</b>	<b>13</b>	<b>5</b>
směna 6-18 a 18-6	11 hod	11 hod
Počet hodin celkem na směnu	143	55
Pracovních dní	23	4356
Dny mimo pracovní dobu	7	770
<b>Počet hodin celkem za měsíc</b>	<b>30</b>	<b>5126</b>

Tab. 1 Harmonogram fyzické ochrany objektu

### 9.4.3 Technická ochrana

#### 9.4.3.1 Elektrický zabezpečovací systém (PZTS)

##### Obsah projektové dokumentace:

###### Písemná část

Je tvořena technickou zprávou vycházející z návrhu systému, obsahuje následující body:

- Všeobecné údaje
- Požadavky na uživatele
- Montáž zařízení PZTS
- Stanovení prostředí
- Požadavky na silnoproudé a slaboproudé rozvody
- Koncepce zabezpečení [10]

###### Výkresová dokumentace PZTS

Slouží především montážním firmám při instalaci systému a rovněž pro účely servisu, revize, prohlídek. Výkresová dokumentace zahrnuje:

- výkres kabelových rozvodů a umístění jednotlivých komponent systému,
- výkresy stavební přípravy,
- bloková a svorková schémata,
- tabulka použitých komponent,
- tabulka použitých kabelů a rozbočovacích krabic,
- kalkulaci energetické spotřeby,
- legendu použitého značení,
- výkresy detailů řemeslného provedení instalace jednotlivých komponent.

Náplň projektové dokumentace PZTS stanovuje – vzhledem ke statutu technických norem – lépe řečeno doporučuje technická normalizační TNI 33 4591-1. [38] Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Návrh systému PZTS – Komentář k ČSN CLC/TS 50131-7:2011 [32]

**Základními etapami zřizování PZTS jsou:**

- návrh systému
- příprava realizace
- montáž PZTS

**Dílčí cíle etapy návrhu systému představují:**

- stanovení rozsahu IHAS,<sup>45</sup>
- volba komponent,
- zpracování návrhu systému.

**Účastníky této etapy jsou:**

- a) objednatel (investor, zadavatel, uživatel),
- b) dodavatel (řešitel, projektant),
- c) provozovatel.

Další potenciálně dotčené subjekty: pojišťovny, Policie ČR, bezpečnostní agentury (napojení na poplachové přijímací centrum), provozovatelé telekomunikačních služeb. [16]

**Podmínky zpracování návrhu odpovídají:**

- 1. provozní náročnosti,
- 2. dislokaci objektu,
- 3. termínu dodávky systému,
- 4. finančním limitům investora.

---

<sup>45</sup> Poplachový zabezpečovací systém ( Intrusion and Hold-up Alarm System).

**Mezi obecné zásady zpracování návrhu systému patří:**

- při zpracování návrhu je třeba dívat se na objekt očima potenciálního pachtatele,
- v závislosti na míře rizika volit komponenty PZTS,
- zohlednit požadavky na základě výsledku bezpečnostního posouzení,
- různé objekty v různých lokalitách můžeme po vyhodnocení zařadit do stejné míry rizika, nicméně se budou lišit, např. počtem a hustotou nasazení komponent PZTS, umístěním komponent, jejich kombinací, zálohováním přenosových cest atd.,
- respektování specifik požadavků na obsluhu,
- zvážení možnosti integrace s nepoplachovými aplikacemi.

**Zásady umístování komponent:**

- respektovat doporučení výrobce k montáži,
- respektovat vlivy prostředí (např. EM rušení, tepelné zdroje, průvan, zvuky atd.),
- minimalizovat plané poplachy vzhledem ke konstrukci a fyzikálním principům komponent PZTS, (především detektory pohybu),
- respektovat požadavky na zabezpečení (např. umístění ústředny PZTS). [14]

Činnost	Dokumentace
montáž	protokol o předání/převzetí pracoviště
oživení	stavební/ montážní deník
prohlídka systému	dokumentace skutečného provedení
funkční zkoušky	protokol o funkční zkoušce
výchozí revize	zpráva o výchozí revizi
proškolení obsluhy	zápis proškolení obsluhy
předání díla	protokol o funkčních zkouškách
zkušební provoz	předávací protokol
předání do trvalého provozu	projekt skutečného provedení
	návod k obsluze, osvědčení o shodě PZTS
	zápis o vyhodnocení zkušebního provozu

Tab. 2 Jednotlivé činnosti projektu a příslušná dokumentace <sup>46</sup>

#### 9.4.3.2 Požární bezpečnost

Pro skladovací prostor naší velikosti budeme muset počítat s tímto vybavením: elektrická požární signalizace, stabilní hasicí zařízení, samočinné odvětrávací zařízení. Z každého místa skladu musí být dosažitelné nejméně dvě únikové cesty vedoucí různým směrem na volné prostranství nebo do chráněné či částečně chráněné únikové cesty. Tyto únikové cesty musí být navrženy tak, aby umožnily požární zásah v kterémkoliv místě skladu alespoň ze dvou stran. Zde budeme aplikovat kromě předepsané legislativy týkající se požární ochrany normu ČSN 73 0845 Požární bezpečnost – sklady [37]. Pro EPS platí norma ČSN EN 54-1. [36]

#### 9.4.3.3 Systém CCTV

Ten bude tvořit velmi důležitou součást celkového zabezpečení a v podstatě nasazení tohoto systému můžeme rozdělit do dvou oblastí. Použití do vnitřního a vnějšího prostředí.

<sup>46</sup> Převzato z: VALOUCH, Jan. *Projektování bezpečnostních systémů*. 1. vyd. Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-230-5.

Z toho také budeme vycházet při návrhu optimálního typu kamer. Primárně se tedy zaměříme na sledování primárních bezpečnostních zón. Těmi budou:

- prostor vjezdu a výjezdu z objektu,
- prostor vstupu do skladu a vstupů do celé budovy (personální vstup, vstup pro řidiče),
- prostor skladu oddělení A (tj. sklad drobné elektroniky),
- prostor příjmu zboží,
- prostor výdeje zboží (expedice).

Pro komplexnost systému nás též zajímají ještě další místa, kde se sledováním CCTV počítáme:

- prostor perimetru obvodové ochrany,
- venkovní komunikace v rámci objektu (pro pěší i autodopravu nebo parkoviště),
- prostor skladu v odděleních B a C,
- chodby v administrativní části budovy,
- prostor určený pro řidiče (tj. kancelář příjmu a výdeje zboží),
- prostor u nakládacích ramp.

V rámci tvorby projektu musíme mít na zřeteli požadavky normy ČSN EN 50 132-x-y (2 a 7), Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích [33]

#### **Hlavními přínosy nasazení CCTV budou:**

- Zvýšení přehledu o situaci v objektu.
- Dostupnost a množství potřebných informací.
- Rychlejší odezva na nestandardní stavy.
- Podpora řešení krizových situací.
- Možnost funkčního propojení nezávislých systémů.

#### 9.4.3.4 *Přístupové systémy*

Před použitím těchto zabezpečovacích prvků nastudujeme soubory norem ČSN EN 50133.

Přístupové systémy (ACS) budou splňovat následující funkce:

- Identifikace.
- Zpracování dat.
- Ovládání přístupového místa.
- Programovatelnost.
- Stavová hlášení.
- Komunikace s ostatními systémy.
- Styk s uživatelem (akustické signály).
- Napájení systému z jednoho přístupového místa.
- Ochrana proti sabotáži, či neoprávněné manipulaci. [34]

Jako identifikační prvky použijeme bezkontaktní čipové karty RFID.<sup>47</sup> Bude použito inteligentní snímací zařízení obsahující paměť přístupových údajů. Provádí rozhodnutí o povolení přístupu samostatně a nezávisle. Komunikace probíhá prostřednictvím sběrnice RS-485.<sup>48</sup> Prostupy budou vyhotoveny v podobě dveří opatřené např. elektromagnety. Pro vstup do skladu bude použit turniket v kombinaci s detekčním rámem.

#### 9.4.3.5 *Napojení na dohledové a poplachové přijímací centrum*

Vycházíme zde z požadavku norem ČSN EN 50-131-1 a její národní přílohy. Dále je provoz PCO<sup>49</sup> upraven normami řady ČSN EN 50 136. [35]

---

<sup>47</sup> Radio-Frequency Identification. Technologie využívající k přenosu mezi čtečkou a čipovým identifikačním médiem (tag) radiových vln.

<sup>48</sup> Standard sériové komunikace.

<sup>49</sup> Pult centrální ochrany

Spojení bude navázáno pomocí sítě GSM, kde bude povinné hlídání napájecího napětí na lince a trvalá kontrola signálu GSM. Pracovník bezpečnostního managementu bude ovládat zařízení pomocí internetového přístupu, kde bude mít možnost nastavit dobu pro uzavření objektu. Zařízení bude automaticky zasílat reporty o stavu systému. Při vzniku poplachu dispečer využít funkce videoverifikace poplachu pro aktuální informaci o skutečném stavu, tím také bude omezen počet planých poplachů.

#### **9.4.4 Plán krizové připravenosti**

dle Metodiky zpracování plánů krizové připravenosti podle § 17 až 18 nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení. [8] [23]

##### **9.4.4.1 ZÁKLADNÍ ČÁST**

- Vymezení předmětu činnosti a úkolů a opatření, které byly důvodem zpracování plánu krizové připravenosti
  - Právní forma, IČ, DIČ, sídlo, statutární orgán.
- Charakteristika krizového řízení
  - Vymezení organizačních částí podílejících se na přípravě na krizové situace a jejich řešení.
  - Předpokládané změny organizační struktury nezbytné k zabezpečení činnosti za krizové situace a plnění opatření vyplývajících z krizového plánu.
  - Krizový štáb.
  - Vazby na příslušné orgány krizového řízení a krizové štáby.
- Přehled a hodnocení možných zdrojů rizik a analýzy ohrožení a jejich možný dopad na činnost subjektu
  - Přehled krizových situací, které mohou ohrozit plnění opatření vyplývajících z Krizového plánu kraje.
  - Přehled dalších možných ohrožení, jež mohou narušit funkci společnosti.

#### 9.4.4.2 OPERATIVNÍ ČÁST

- Přehled opatření vyplývajících z Krizového plánu kraje a způsob zajištění jejich provedení:
  - Například zabezpečení vlastního fungování za krizových situací, nebo zabezpečení nouzového zásobování pitnou vodou v krizových situacích nebo zabezpečení nouzového zdroje elektrické energie v krizových situacích, atd.).
- Způsob zabezpečení akceschopnosti subjektu pro zajištění provedení krizových opatření a ochrany činnosti subjektu:
  - Zde naše společnost uvede vlastní postup, kterým zajistí realizaci činností, které jí byly uloženy.
  - Určí odpovědnou osobu za realizaci opatření.
  - Požadavky na síly a prostředky, které společnost bude potřebovat k zajištění požadovaných úkolů.
  - Příklad: způsob požárního zabezpečení, vstupní/výstupní režim osob, obsluha bezpečnostních systémů, evidence vjezdu/výjezdu motorových vozidel, kamerový systém apod.
- Postupy řešení krizových situací a mimořádných událostí identifikovaných v analýze ohrožení:
  - Vyznačení dopadů na fungování subjektu.
  - Plánované opatření pro zvládnutí situace.
  - Určení odpovědné osoby.
  - Požadavky na síly a prostředky v rámci subjektu.
  - Příklad: Narušení hrází významných vodohospodářských děl se vznikem zvláštní povodně.
- Přehled spojení na příslušné orgány krizového řízení.
  - Například na bezpečnostní management, který bude tvořit s vedení společnosti krizový štáb organizace (mobil, e-mail).

- Přehled plánů zpracovávaných podle zvláštních právních předpisů využitelných při řešení krizových situací.
  - Zde budou uvedeny jednotlivé plánovací dokumentace, jména zhotovitelů a místo uložení listinné podoby, například evakuační plány.

#### **9.4.4.3 POMOCNÁ ČÁST**

- Přehled právních předpisů využitelných při přípravě na mimořádné události nebo krizové situace a jejich řešení.
  - Smlouvy s krajem nebo všemi subdodavateli.
- Přehled uzavřených smluv k zajištění provedení opatření, které byly důvodem zpracování plánu krizové připravenosti.
- Zásady manipulace s plánem krizové připravenosti.
- Geografické podklady v součinnosti s Hasičským záchranným sborem kraje.
- Další dokumenty související s připraveností na mimořádné události nebo krizové situace a jejich řešením.
  - Statut, smlouvy a složení krizového štábu společnosti. [43]

#### **9.4.5 Zpracování typových plánů**

Na základě těchto požadavků bezpečnostní management zpracuje jednotlivé typové plány pro situace:

- Živelních pohrom (úder blesku na objekt, sněhová kalamita, bouře).
- Zvýšení hladin okolních toků s rizikem povodně.
- Epidemie – hromadné nákazy osob.
- Přerušování dodávek elektrické energie.
- Přerušování dodávek plynu a tepelné energie.
- Únik provozních kapalin v okolí objektu.
- Závažné narušení dopravní obslužnosti vlivem hromadné nehody.

**Plány budou obsahovat:**

- Stručný popis krizové situace.
- Dopady krizové situace.
- Podmínky (předpoklady) pro řešení krizové situace.
- Doporučené typové postupy, zásady a opatření pro řešení krizové situace.
- Podklady pro vypracování, které obsahují odborné údaje, technické údaje, organizační údaje.
- Identifikaci zpracovatele typového plánu.

**9.5 ORGANIZOVÁNÍ ČINNOSTÍ****9.5.1 Motivování a stimulování**

Bezpečnostní management musí získat prostředky k angažovanosti vedení společnosti, které by bylo dobře informované o zaváděných systémech a seznámilo se s pozitivními dopady těchto opatření. Směrem k zaměstnancům musí představit zjednodušení systému, všechny zaměstnance proškolit a vysvětlit jim důvody, které vedou bezpečnostní management k těmto krokům v bezpečnostním plánování. Bezpečnostní management nepodněcuje diskuze a zajímá se o názory ze všech profesních skupin společnosti. Cílem by měl být pocit bezpečného prostředí při vykonávání pracovní činnosti.

**9.5.2 Koordinování a operativní řízení**

- Bezpečnostní management plně spolupracuje na dokončovacích pracích, instalacích technologií, zaškolení odborných pracovníků ze strany dodavatelů technologií.
- Sleduje postup a aktuální legislativu pro nasazení těchto technologií.
- Vedení společnosti organizuje přesun zboží a naskladnění.
- Příprava a zkoušky nového skladového systému.
- Společnost vyčlení 10 dní na kompletní doladění všech prací, v tuto dobu nepřijímá žádné objednávky.
- Zákazníky o tomto kroku včas informuje.
- Spolupráce na krizových plánech s HZS kraje.

- Nastavení kontrolních procedur.
- Návčik evakuačních plánů.

## 9.6 HODNOCENÍ VÝSLEDKŮ

### 9.6.1 Zjišťování fakt

- Systém zabezpečení je adekvátní požadavkům, které byly vysloveny v zadání.
- Vlivem doladřování systému se vyskytly případy falešných poplachů.
- Problematické situace před vjezdem do areálu, byla posílena sestava strážní služby.
- Docházelo k časovým skluzům při plnění jednotlivých bodů.

### 9.6.2 Kritické posouzení

Hodnotíme například vhodnost nasazení technických prostředků zajišťujících bezpečnost či efektivitu režimových opatření. Zde také hodnotíme časové hledisko – zda jsme stihli všechny úkoly v předpokládaných termínech, pokud se tak nestalo, co bránilo jejich včasnému splnění. Další hodnotou pro kritické posouzení by byly například otázky typu: Bylo naše počínání dobře materiálně podpořeno ze strany vedení? Je vše v legislativním souladu? Co bylo z naší strany špatně vysvětleno? Významný vliv na celkový projekt může mít také otázka určení správných priorit. Vždy se snažíme hledat chyby na své straně, abychom při našem dalším počínání mohli postupovat lépe a zařadit naše chyby jako zkušenosti ve vytváření následujících projektů.

### 9.6.3 Návrh opatření

Mezi tyto návrhy mohou patřit například nastavení termínu pro zkušební provoz detektorů za účelem předcházení falešným poplachům. Tyto návrhy slouží k případným korekcím jednotlivých negativních vlivů a jejich uvedení do předpokládaného stavu. Zde si stanovíme harmonogram pravidelných kontrol všech prvků zapojených do bezpečnostního systému.

### 9.6.4 Uplatnění zkušeností z praxe

Zde osoba, která zpracovává bezpečnostní plán, může při řešení otázek kritického posouzení využít svých zkušeností, jež v minulosti pomohly vyřešit nedostatky či odchylky v bezpečnostním plánování. Nedá se však jednoznačně vše zobecnit, každý projekt totiž

má svá specifika. Důležité je však přesné dodržení plánu činností a před těmito kroky kvalitní analýza současné situace. Je dobré vysvětlit vedení podniku, aby neřídilo několik zásadních změn najednou. Vždy si vymezit cíl a naplnit jeho kvalitativní požadavky. V oblasti řízení bezpečnosti jsou tyto otázky řízení klíčové.

## 9.7 PLÁNOVACÍ SOFTWARE JAKO NÁSTROJ PRO ŘÍZENÍ PROJEKTU

Praktickým pomocníkem při plánování může být týmu bezpečnostního managementu například software Microsoft Project Professional. Po otevření nového projektu zadáme požadované úkoly a fáze, které můžeme ještě rozřídít do skupin (tzv. souhrn). K jednotlivým úkolům přiřadíme časové údaje, které nám omezují dobu na vykonání úkolu. Mezi úkoly vytvoříme závislosti a definujeme zdroje, jenž nám pomohou k dosažení úkolu. Poté můžeme zobrazit první výstup a tím je časová osa. Software dále umožňuje zpracování postupu plánování do těchto zobrazení:

- Ganttův diagram.
- Sledovací Ganttův diagram, kde v reálném čase sledujeme průběh projektu a procentuální plnění.
- Formulář úkolů nám rozdělí jednotlivé činnosti na čas potřebný k vykonání činnosti a zohlední případná zpoždění.
- Formulář zdrojů je seznam všech účastníků projektu a zobrazí mimo jiné počet odpracovaných hodin a termíny činností jednotlivých zdrojů.
- Kalendář úkolů nám přehledně zobrazí plánované činnosti na jednotlivé dny.
- Zobrazí postup plánování do síťového diagramu.
- Seznam úkolů v jednotlivých etapách plánování.

V přílohách jsou uvedeny výstupy ze softwaru pro daný modelový příklad v bezpečnostním plánování.

## 9.8 KONTROLNÍ SEZNAM A PŘÍSTUPY K JEHO VYUŽITÍ BEZPEČNOSTNÍM MANAGEMENTEM

Kontrolní seznam (checklist) může sloužit jako nástroj pro kontrolu a dodržování pravidel z pohledu bezpečnosti. Jde o jednoduchý a účinný nástroj. Obsahuje sto bodů kontrolovacích oblastí, které se hodnotí podle toho, zda bod vyhovuje či nikoli. Celkový počet dosažených bodů bude znamenat výsledek aktuálního zkoumaného stavu. Tento proces by se měl opakovat v pravidelných cyklech, aby se dokázalo, zda jsou všechny požadavky zaměstnanci dodržovány.

- 0 – 20% stav naprosto nedostatečný, nevyhovující,
- 21 – 40 % stav nedostatečný, závažné nedostatky zásadního charakteru,
- 41 – 60 % stav nedostatečný, mnoho závad,
- 61 – 80 % menší závady,
- 81 – 99% nepodstatné závady,
- 100 % bez závad.

Příklad kontrolního seznamu pro bezpečnostní management je součástí přílohy.



Obr. 19 Centrální sklad společnosti Alza.cz<sup>50</sup>

## 9.9 Neustálý rozvoj a zpětná vazba

Uvedením systému do provozu práce managementu na bezpečnostním plánování rozhodně nekončí. Důležité body řízení bezpečnostního managementu:

- Výběr takových témat benchmarkingu, která jsou velmi úzce spojena s vašimi aktuálními cíli a prioritami. Zaměření se v benchmarkingu na jeden či dva aspekty činnosti ročně.
- Začlenit do otázek strategický přístup, ptát se na příčiny pokroku, zvažování způsobu zlepšení apod.
- Ujasnit si cíle benchmarkingu – co musí být naplněno, jaké otázky mají být zodpovězeny, jaké oblasti musí být probádány, apod.

---

<sup>50</sup> Převzato z: *Alza.cz: Oddělení logistiky* [online]. [cit. 2014-05-20]. Dostupné z: <http://www.alza.cz/article/oddeleni-logistiky-art7657.htm>

- Porozumět vlastním procesům. Výběr dobrých partnerů pro porovnání vyžaduje hluboké porozumění vlastním procesům i průběhu benchmarkingu.
- Podpora nejvyššího vedení v realizaci benchmarkingu je velmi důležitá a organizace, kde je podpora na vysoké úrovni, vykazují vyšší provozní i finanční přínosy benchmarkingu.
- Pečlivý výběr pracovníků, kteří budou začleněni do benchmarkingu. Ujistit se, že jsou si vědomi toho, co je od nich očekáváno.
- Mít připravené kontakty na své partnery, přemýšlet o jejich zájmech při poskytování zpětné vazby.
- Dodržení realizace tří základních kroků benchmarkingu: srovnávací analýza, návrh nových procesů, implementace. Častou chybou je provedení pouze srovnávací analýzy.

Samozřejmě, že benchmarking není jediný způsob zpětné vazby bezpečnostního managementu. Jsou to kontrolní mechanismy jako je externí či interní audit, miniaudit, kontrolní seznamy nebo bezpečnostní prověrky pro zjištění aktuálního stavu a neustálé zlepšování.

## ZÁVĚR

Bezpečnostní plánování má ve svém portfoliu obrovský záběr činností, jež se prolínají několika odvětvími lidské činnosti. Byly zmíněny a popsány všechny podstatné výchozí body, které na činnost plánování mají vliv i ty, které na něj navazují. Popis metody se ubíral spíše technologickým směrem, protože technickými otázkami při návrzích se zabývá spíše oblast bezpečnostního projektování. Mezi dílčí kroky bezpečnostního plánování patří též bezpečnostní politika. Ta je pro další činnosti velmi důležitá. Mnoho firem však do dnešní doby žádný takový koncept vypracovaný nemá. Není tedy nutné čekat do prvního bezpečnostního incidentu, ale bezpečnostní politiku je vhodné aplikovat preventivně. Je to však výborný prostředek, na němž stojí celý systém bezpečnosti. Podstatou plánování je též tvorba několika variant pro určení směru kam se má plánování odebrat. Pro organizaci to však znamená obklopit se dobrým týmem v čele s kvalifikovaným bezpečnostním manažerem. Ten pro organizaci zpracuje postupy, které vedou k minimalizaci rizik a to za pomoci bezpečnostního plánování a expertizy. Neexistuje však sterilní prostředí, kde bychom pravděpodobnost snížili na nulovou hodnotu. Narušitelé s jakýmkoliv cílem budou vždy o krok před námi, cílem však bude vytvoření aparátu, jenž nám určí cestu jak rizikům předejít, nebo případně jak je dobře zvládnout. K prioritám těchto kroků tedy bude patřit ochrana života, zdraví, majetku ať hmotného či nehmotného a také ochrana životního prostředí. Takové postupy by tedy měly být cílem bezpečnostního plánování pro organizace podnikající v privátní praxi. Dále je důležité hledat stále nová řešení a minimalizovat hrozby. V našem případě je nutné plány stále aktualizovat a nespokojit se s vyhotovením, které postupem času může být zastaralé. Organizace působící v privátní praxi by proto na tyto činnosti oboru průmyslu komerční bezpečnosti neměli zapomínat a implementovat je do své činnosti. Pozice kvalifikovaného bezpečnostního managementu v organizaci je zcela klíčová a bezpečnostní plánování bude tvořit základní kámen dalších činností v oblasti bezpečnosti.

## SEZNAM POUŽITÉ LITERATURY

### Monografické publikace

- [1] ALDAG, Ramon J. *Management*. 2. vyd. Cincinnati (Ohio): College Division, 1991. ISBN 978-053-4985-189.
- [2] BRABEC, František. *Ochrana bezpečnosti podniku*. EUROUNION, s.r.o., Praha 1996, ISBN 80-85858-29-0.
- [3] BRABEC, František a kolektiv. *Bezpečnost pro firmu, úřad, občana*. Praha, Public History, 2001, ISBN 80-86445-04-6.
- [4] ELBEL, Jaromír. *Systém vnitřního řízení bezpečnosti v podniku*. Část 1, Metodický návod k zavedení systému. Praha, Český úřad bezpečnosti práce, 1998, ISBN 80-901654-5-1.
- [5] FUCHS, Pavel a VALIŠ, David. *Metody a analýzy řízení rizika*. Technická univerzita v Liberci. 1. vyd. Liberec, 2004.
- [6] GRASSEOVÁ, Monika, BRECHTA, Bohumil. *Efektivní rozhodování: analýzování, rozhodování, implementace a hodnocení*. 1. vyd. Brno: Edika, 2013. ISBN 978-80-266-0179-1.
- [7] JAŠEK, Roman a MALANÍK David. *Bezpečnost informačních systémů*. Fakulta aplikované informatiky. 1. vyd. Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 978-80-7454-312-8.
- [8] KARDA, Ladislav a KUDLÁK Aleš. *Analýza, metody a nástroje řešení krizových situací*. Jihočeská univerzita v Českých Budějovicích. České Budějovice, 2007.
- [9] KERZNER, Harold C. *Using the Project Management Maturity Model: Strategic Planning for Project Management*. 2. vyd. 2005. ISBN 978-0-471-69161-7.
- [10] KINDL, Jiří. *Projektování bezpečnostních systémů I*. 2. vyd. Zlín: Univerzita Tomáše Bati, 2007. ISBN 978-80-7318-554-1.
- [11] LAUCKÝ, Vladimír a DRGA, Rudolf. *Speciální technologie komerční bezpečnosti*. 1. vyd. Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-146-9.

- [12] LAUCKÝ, Vladimír. *Řízení technologických procesů v průmyslu komerční bezpečnosti*. 2. vyd. Ve Zlíně: Univerzita Tomáše Bati, 2006. Učební texty vysokých škol. ISBN 80-7318-432-X.
- [13] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II*. 2. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. 123 s. ISBN 978-80-7318-631-9.
- [14] LUKÁŠ, Luděk a kol. *Bezpečnostní technologie, systémy a management I*. 1. vyd. Zlín: VeRBuM, 2011. ISBN 978-80-87500-05-7.
- [15] LUKÁŠ, Luděk a kol. *Bezpečnostní technologie, systémy a management II*. 1. vyd. Zlín: VeRBuM, 2012. ISBN 978-80-87500-19-4.
- [16] VALOUCH, Jan. *Projektování bezpečnostních systémů*. 1. vyd. Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-230-5.
- [17] YEATES, Donald a CADLE James. *Business analysis*. 2. vyd. London: British Computer Society, 2010. ISBN 978-190-6124-618.

#### **Legislativní dokumenty**

- [18] Česká republika. Zákon o trestním řízení soudním (trestní řád): 141/1961 Sb.
- [19] Česká republika. Zákon o státním odborném dozoru nad bezpečností práce: 174/1968 Sb.
- [20] Česká republika. Zákon o ochraně utajovaných skutečností a o změně některých zákonů: 148/1998 Sb.
- [21] Česká republika. Vyhláška Národního bezpečnostního úřadu o objektové bezpečnosti: 339/1999 Sb.
- [22] Česká republika. Zákon o ochraně osobních údajů a o změně některých zákonů: 101/2000 Sb.
- [23] Česká republika. Zákon o krizovém řízení a o změně některých zákonů (krizový zákon): 240/2000 Sb.
- [24] Česká republika. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: 412/2005 Sb.
- [25] Česká republika. Zákoník práce: 262/2006 Sb.

[26] Česká republika. Občanský zákoník: 89/2012 Sb.

### Normy

[27] ČSN EN ISO 9000. *Systémy managementu kvality - Základní principy a slovník*. 2006. vyd.

[28] ČSN EN ISO 9004. *Řízení udržitelného úspěchu organizace - Přístup managementu kvality*. 2010. vyd.

[29] ČSN ISO 31000. *Management rizik - Principy a směrnice*. 2010.

[30] ČSN EN ISO 14001. *Systémy environmentálního managementu - Požadavky s návodem pro použití*. 2005.

[31] ČSN EN 15221. *Facility management - Část 1: Termíny a definice*. 2014. vyd.

[32] ČSN EN 50131-1 ed. 2. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. 2007. vyd.

[33] ČSN EN 50132. *Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích*. 2002. vyd.

[34] ČSN EN 50133. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích*. 2001. vyd.

[35] ČSN EN 50136. *Poplachové systémy - Poplachové přenosové systémy a zařízení*. 2012. vyd.

[36] ČSN EN 54-1. *Elektrická požární signalizace - Část 1: Úvod*. 2011.

[37] ČSN 73 0845. *Požární bezpečnost staveb - Sklady*.

[38] TNI 33 4591-1. *Poplachové systémy - poplachové zabezpečovací a tísňové systémy. Příloha 1 - Návrh systému PZTS - komentář k ČSN CLC/TS 50131-7:2011: Technické normalizační informace*. 2012.

### Internetové zdroje

[39] *Alza.cz: Oddělení logistiky* [online]. [cit. 2014-05-20]. Dostupné z: <https://www.alza.cz/article/oddeleni-logistiky-art7657.htm>

[40] *Česká společnost pro jakost: Benchmarking* [online]. 2014 [cit. 2014-05-19]. Dostupné z: <http://www.csq.cz/benchmarking/>

- [41] Metoda analýzy FTA. *Ikvalita.cz: Portál pro kvalitáře* [online]. [cit. 2014-05-01]. Dostupné z: <http://www.ikvalita.cz/tools.php?ID=52>
- [42] *ICVV: Realizace projektu* [online]. 2012 [cit. 2014-05-20]. Dostupné z: <http://www.icvv.cz/realizace>
- [43] *Portál krizového řízení pro Jihomoravský kraj* [online]. 2013 [cit. 2014-05-10]. Dostupné z: <http://krizport.firebrno.cz/>
- [44] *Podnikátor: Jakost a požadavky na jakost* [online]. 2014 [cit. 2014-05-11]. Dostupné z: <http://www.podnikator.cz/provoz-firmy/management/rizeni-podniku/n:16565/Jakost-a-pozadavky-na-jakost>
- [45] *QM Profi: Analýza stromu událostí* [online]. 2014 [cit. 2014-05-21]. Dostupné z: <http://www.qmprofi.cz/33/analyza-stromu-udalosti-eta>
- [46] *Úrad vlády SR: Centrálný register zmlúv* [online]. [cit. 2014-05-12]. Dostupné z: <http://www.crz.gov.sk/>
- [47] *National Safety Council: Safety Management Systems* [online]. 2014 [cit. 2014-05-15]. Dostupné z: [http://www.nsc.org/safety\\_work/benchmarking\\_measurement/Pages/benchmarking\\_measurement.aspx](http://www.nsc.org/safety_work/benchmarking_measurement/Pages/benchmarking_measurement.aspx)

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

ACS	Access Control System
BOZ	Bezpečnost a ochrana zdraví
BOZP	Bezpečnost a ochrana zdraví při práci
CCA	Cause-Consequence Analysis
CCTA	Central Computer and Telecommunications Agency
CCTV	Closed Circuit Television
CD	Compact Disc
CRAMM	CCTA Risk Analysis and Management Method
ČSN	Česká technická norma
DIČ	Daňové identifikační číslo
DVD	Digital Video Disc
EM	Elektromagnetické
EN	Evropská norma
ETA	Event Tree Analysis
FTA	Fault Tree Analysis
GPS	Global Position System
GSM	Global System for Mobile Communications
HW	Hardware
HZS	Hasičský záchranný sbor
IČ	Identifikační číslo
IHAS	Independent Healthcare Advisory Services
IS	Informační systém
ISMS	Information security management system
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria

---

IZS	Integrovaný záchranný systém
LAN	Local Area Network
NBÚ	Národní bezpečnostní úřad
PC	Personal Computer
PCO	Pult centrální ochrany
PERT	Project Evaluation and Review Technique
PEST	Political, Economic, Social and Technological analysis
PZTS	Poplachové zabezpečovací a tísňové systémy
RFID	Radio Frequency Identification
SPZ	Státní poznávací značka
SW	Software
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TCSEC	Trusted Computer System Evaluation Criteria
TNI	Technická normalizační informace
USB	Universal Serial Bus
VLAN	Virtual LAN

**SEZNAM OBRÁZKŮ**

Obr. 1	Vztah míry zabezpečení na míře ohrožení	14
Obr. 2	Proces zpracování bezpečnostní expertizy	16
Obr. 3	Proces bezpečnostního plánování	30
Obr. 4	Diagram analýzy SWOT	37
Obr. 5	Parettův diagram	40
Obr. 6	Krizová matice podle Klause Winterlinga	41
Obr. 7	Analýza FTA	43
Obr. 8	Analýza ETA	44
Obr. 9	Išikavův diagram	45
Obr. 10	Znázornění příčin nedostatečného fungování bezp. systému organizace	48
Obr. 11	Prognostický proces	54
Obr. 12	Proces řízení rizik	58
Obr. 13	Vztah bezpečnostní politiky a celkové politiky organizace	65
Obr. 14	Prvky vnitřního řízení společnosti	74
Obr. 15	Struktura společnosti	83
Obr. 16	Analýza současného stavu	99
Obr. 17	Bezpečnostní posouzení	111
Obr. 18	Kontrola vjezdu do objektu	115
Obr. 19	Centrální sklad společnosti Alza.cz	132

**SEZNAM TABULEK**

Tab. 1 Harmonogram fyzické ochrany objektu	119
Tab. 2 Jednotlivé činnosti projektu a příčinná dokumentace	123

## SEZNAM PŘÍLOH

Příloha P1: Kontrolní seznam

Příloha P2: Ganttův diagram

Příloha P3: Časová osa

Příloha P4: Týmový plánovač

Příloha P5: Síťový diagram

Příloha P6: Kalendář úkolů