Metodika a proces zpracování bezpečnostní analýzy

Metodology and the creating process of security analysis

Bc. Radek Pšenka

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Bc. Radek PŠENKA**
Osobní číslo:	**A09391**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Metodika a proces zpracování bezpečnostní analýzy**

Zásady pro vypracování:

1. **Zpracujete rešerši literatury, která se vztahuje k tématu DP.**
2. **Vymezte pojem bezpečnostní analýza a její význam pro ochranu podnikatelských objektů a dalších bezpečnostních zájmů.**
3. **Definujte metodiku a proces zpracování bezpečnostní analýzy.**
4. **Zpracujte kompletní bezpečnostní analýzu pro konkrétní podnik (společnost, firmu).**
5. **Zpracujte ekonomickou rozvahu k vyhotovené bezpečnostní analýze.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **SMEJKAL, Vladimír, RAIS Karel, Řízení rizik ve firmách a jiných organizacích. GRADA Publishing, 2009. ISBN: 978-80-247-3051-6**
2. **VALOUCH, Jan: Projektování integrovaných systémů. (přednáška) Zlín : UTB FAI, 2010.**
3. **BRABEC, F. a kol.: Bezpečnost pro firmu, úřad, občana. Public History, Praha 2001. ISBN 8086445046.**
4. **LAUCKÝ, Vladimír: Technologie komerční bezpečnosti II. Zlín: Univerzita Tomáše Bati, 2007. ISBN 978-80-7318-631-9.**
5. **LAUCKÝ, Vladimír: Technologie komerční bezpečnosti I. Zlín: Univerzita Tomáše Bati, 2003. ISBN 80-7318-119-3.**
6. **LAUCKÝ, Vladimír, HURTA, Josef: Management bezpečnostního inženýrství. Zlín: Univerzita Tomáše Bati, 2006. ISBN 80-7318-412-5.**
7. **Seznam, Přehled metodik pro analýzu rizik. [Pomůcka, metodika]. Praha: Ministerstvo vnitra, Generální reditelství HZS ČR, č.j.: PO-58-7/PLA-2004. dostupné na www.mvcr.cz**
8. **Security magazín, Praha: FAMily media, s.r.o., r. 2007-2011.**

Vedoucí diplomové práce: **PhDr. Mgr. Stanislav Zelinka**
Ústav bezpečnostního inženýrství

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

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

Ve Zlíně dne 25. února 2011

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

V této práci je shrnuta problematika bezpečnostní analýzy pro ochranu objektů, tím rozumíme odhalení souvislostí a rozbor stavu zkoumaného objektu z hlediska bezpečnosti. Práce popisuje nejběžnější metody analýzy, stejně jako uvádí konkrétní příklady pro lepší pochopení a srozumitelnost textu. V praktické části je na základě poznatků z teorie zpracována bezpečnostní analýza konkrétního podniku, pro ukázku aplikace metod v praxi.

Klíčová slova: bezpečnostní analýza, analýza rizik, hrozba, riziko, protiopatření

ABSTRACT

This document summarizes the problem of security analysis for the protection of objects, which means discovery of connections and dissection of security state. The work describes the most common methods of analysis, as well as concrete examples for better understanding and clarity of the text. In the practical part, the safety analysis of a particular company was made, based on the findings from the theory part of this document, to show the application of methods in practice.

Keywords: security analysis, risk analysis, threat, risk, countermeasure

Chtěl bych tímto poděkovat především vedoucímu práce PhDr. Mgr. Stanislavu Zelinkovi a JuDr. Vladimíru Lauckému.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

Slovo analýza pochází z řeckého ana-lyó a znamená rozklad či rozbor. Myslí se tím rozdělení složitějšího problému na jednodušší části a tím usnadnění pro jeho poznání. Bezpečnostní analýzou pak rozumíme analýzu bezpečnostního stavu, neboli úrovně bezpečnosti. V běžném životě se setkáváme s procesem analýzy častěji, než si uvědomujeme. Analýzu všeho kolem sebe provádíme neustále, abychom měli základ pro naše budoucí rozhodnutí. Jelikož je ale v našem případě analýza pojmuta vědecky, musíme dodržovat určitý postup. Využít lze třeba učený odhad, tento odhad však, jak ostatně vyplývá z názvu, je odhadem na základě znalosti a nikoliv již pouhé domněnky, jako v běžném životě. Správně stanovit bezpečnostní rizika je velmi těžká úloha, u které vynikají osoby, mající tzv. "bezpečnostní čich"[1]. Pro profesionální přístup k analýzám jsou rozpracovány různé metodiky a postupy, které mají svá konkrétní pravidla. Každá metoda má svá specifika a je více či méně vhodná pro řešenou situaci. Výběr metody může někdy radikálně ovlivnit výsledek a tím i přínos analýzy. Je proto vhodná určitá zkušenost s tvorbou analýz, aby nedocházelo k plýtvání časem a prostředky na analýzu, jejíž typ nám neposkytne požadované informace, a co hůř, můžeme z ní mít pocit falešného bezpečí.

Téma bezpečnostní analýzy není nijak nové, a proto bylo již zpracováno v některých publikacích. Zejména úvodní část analýzy rizik, která je podrobně zpracována i na internetu. Pro ostatní části analýzy je vhodné využít tištěné zdroje. Přesto jsou tyto publikace či články fragmentovány a popisují většinou jen určitou část procesu analýzy. Kompletní souhrn problematiky obsahuje tato práce. Rešerše literatury a zdrojů, vztahujících se k tématu, je tvořena rejstříkem na konci této práce.

[1] Jde o nadání nebo talent popsat a správně provést analýzu bezpečnostní situace, kdy výsledek vede k úspěšnému vyřešení této situace. Podle JuDr. Lauckého je tento čich určitým šestým smyslem při rozkrývání souvztažností a je tedy vrozen, nedá se naučit. S tímto se ztotožňuji, stejně jako s tvrzením, že tento čich má mizivé procento obyvatel.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ ANALÝZA

Pojem bezpečnostní analýza (dále jen BA) není zcela jednoznačný, a proto se v této práci pokusím o jeho kompletní popis. Obecné rysy BA byly popsány v úvodu, nelze však stanovit obecný postup, ten je odlišný vždy dle požadavků konkrétní situace. V praxi se ale setkáme se dvěma základními typy, které se od sebe liší, jsou to:

- BA prováděná samotnou firmou za účelem identifikace a řízení rizik v podniku.

  Bezpečnostní politika každé firmy stanoví, co je pro ni prioritní a jaké zájmy chce především chránit. Někdy může být provedení BA dokonce obligatorní, například v případě chemických provozů, kdy je vyžadována zákonem pro prevenci technologických havárií. Bezpečnostní politika nám tedy určuje směr jakým se vydat, a forma, kterou k tomu zvolíme, už závisí na nás.

- BA prováděná bezpečnostními agenturami za účelem přípravy na ochranu objektu,

  popřípadě jako forma poradenství, kdy se po předání výstupů analýzy zákazník sám rozhodne, zda investovat do zlepšení zabezpečení, či ne. Před návrhem ochrany objektu a jiných bezpečnostních zájmů subjektů bychom měli vždy provést profesionální analýzu, pokud máme zájem o maximální funkčnost námi následně provedených bezpečnostních opatření. Zároveň v případě, kdy dojde ke změně podmínek, se kterými analýza pracovala, či již zavedená bezpečnostní opatření selžou, je vhodné analýzu revidovat. V podstatě tato BA spadá pod analýzu prováděnou samotnou firmou, jelikož pokud vyžaduje ochranu objektu agenturou bezpečnostní politika, vedení firmy tento úkol agentuře zadá. Poté se zpracovává bezpečnostní prognóza a následně konkrétní plán opatření. BA je také vhodné provést při zjištění vážných nedostatků ochrany a ostrahy objektu a při změně hlídací agentury. Této BA jsem se podrobněji věnoval v kapitole 4.

Může být prováděna též bezpečnostní analýza subjektu, neboli osoby, pokud je naším oborem bodyguarding, ovšem to uvádím pouze pro kompletní přehled, téma této práce se zabývá objektovými analýzami.

BA je obecně metodou zkoumání pomocí defragmentace objektu na základní prvky, kdy se hledají možnosti vnitřní zranitelnosti, vnějších hrozeb a zavedených bezpečnostních opatření. Cílem analýzy je detekce maximálního počtu činitelů zranitelnosti a

bezpečnostních mezer zkoumaného objektu, odhad hrozeb, rizik a případné negativní dopady na zkoumaný objekt, určení efektivnosti současných bezpečnostních opatření a návrh jejich inovace pro maximální omezení rizik na přijatelnou hodnotu. Snažíme se tedy odhalit možná rizika a pomocí prevence předejít jejich vzniku. Vždy je totiž snazší aplikovat preventivní opatření a sledovat, jak zabránily vzniku škody, než odstraňovat následky a sčítat škody. Investice do BA a protiopatření tudíž není zejména u větších firem vyhazováním peněz, ale naopak ochranou proti kolapsu podniku. Pro lepší pochopení celkové problematiky BA je vhodné uvědomit si základní logická paradigmata: Anylýzu provádíme pro zamezení ztrát či jejich minimalizaci. Provádíme ji v okamžiku, kdy nebezpečí hrozí přerůst v hrozbu. Středem naší pozornosti při analýze jsou procesy, subjekty, majetek a stav zabezpečení. Analýzu provádíme nástroji analýzy (viz. 3), tedy nikoliv použitím neseriózních metod. Analýzu provádíme sami osobně nebo prostřednictvím specializované firmy. Cílem BA je vyhodnotit stav zabezpečení a odpovědět na otázku, zda je dostačující.

Zájmy, které chceme ochraňovat, se mohou u různých podniků lišit a u každého mohou mít jinou prioritu, což vychází vždy z bezpečnostní politiky podniku. Lze je rozčlenit do několika základních kategorií:

- Ochrana hmotného majetku (objekty, prostory, výrobní zařízení, pracovní pomůcky a potřeby, materiál, hotové výrobky, zásoby, polotovary).
- Ochrana nehmotného majetku (jde o obchodní, výrobní, provozní informace, dále ochrana dat získaných výzkumem, vynálezy, informace o koncepčním rozvoji, licenční práva, patenty a vynálezecká práva, zlepšovací návrhy, know-how, osobní informace).
- Ochrana osob (majitelé a spolumajitelé podniku mohou být terčem vydírání, ale musí nás zajímat i ochrana pracovníků, potencionálně i návštěvníků provozu, dále obchodní partneři, vedoucí podniku).
- Ochrana veřejného pořádku a bezpečnosti v podniku (režimová opatření v objektu, latentní kriminalita, podnikoví detektivové zasahující vůči narušování technologických postupů nebo sabotáží k vyvolání havárie či poruchy).
- Ochrana bezporuchovosti provozu podnikatelských aktivit (především elektronická kontrola poruch nebo ochrana pomocí firemních detektivů).

- Protipožární ochrana objektů firmy (režimová opatření, kontrola funkčnosti zařízení, požární cvičení pro zaměstnance, protipožární hlídky, případně podnikoví hasiči, samozřejmostí je vybavení hasicími přístroji, případně EPS).
- Ochrana bezpečnosti a zdraví při práci a pracovní hygieny, někdy opomíjená kategorie. Špatné pracovní podmínky mohou vytvořit nespokojeného zaměstnance toužícího po odvetě vůči podniku. Především však zajištěním tohoto faktoru napomáháme k bezporuchovosti provozu a k minimalizaci lidských selhání. Především režimová opatření a jejich kontrolní mechanismy.
- Ochrana enviromentální (opět režimová opatření, případně tato ochrana zahrnuta v politice podniku, hlásiče provozních poruch jako únik plynu, ropných látek či jiných nebezpečných látek).

BA je tedy souhrn ucelených poznatků a informací o konkrétním objektu, situaci či jevu z bezpečnostního hlediska, který má zásadní význam pro správnou funkci podniku. Jde o proces, ve kterém hledáme v množině informací podstatná fakta a skutečnosti, ovlivňující bezpečnost objektu či subjektu. Ta následně třídíme a srovnáváme je s ostatními informacemi tak, abychom mohli učinit logické závěry. Východisky BA jsou:

1.1 Stupeň účinnosti

Pokud předpokládáme určitou účinnost ochrany, bude její stupeň závislý na těchto faktorech:

1.1.1 Úroveň komplexnosti

Komplexnost neboli celistvost bude odvislá od složení:

- Fyzické ochrany – pracovníci ochrany, psovodi se psy.
- Technické ochrany – MZS, EPS, PZTS, CCTV.
- Tzv. vnitřní ochrany – podnikoví detektivové provádějící podnikovou kontrašpionáž a špionáž.
- Na provázanosti mezi těmito typy ochran. Jelikož sebelepší technické prostředky jsou neúčinné bez adekvátní odezvy člověka na poplachový signál.

1.1.2 Úroveň komfortu

Od vyšší úrovně komfortu je odvozena vyšší cena a naopak. Komfort ovlivňuje stav (počet, profesionalitu) fyzické ochrany, technických prostředků a vnitřní (detektivní) ochrany.

1.1.3 Úroveň vybavení a profesionalita

Týká se výstroje a výzbroje, spojovacích prostředků, atd. Vztahuje se k osobám provádějícím fyzickou ochranu, montáž a servis techniky, výjezdovým skupinám na PCO a firemním detektivům.

1.1.4 Optimalizace rozsahu a kvality dokumentace

Míněno dokumentace, vztahující se k bezpečnosti firmy. Patří sem:

- Řád výkonu služby, což je dokument subjektu zajišťujícího ochranu firmy, může jím být agentura nebo i firma samotná.
- Směrnice výkonu služby, kde je obecně charakterizován objekt, vyhodnocena riziková místa, popsáno umístění strážních stanovišť a technického zabezpečení firmy. Pak povinnosti strážných, zásady pro součinnost s policií, bezpečnostním technikem, podnikovými detektivy, vedením objektu a povinnosti z hlediska protipožární ochrany. Zásady pro spojení s objektem, stejně jako vyrozumění určených osob při mimořádné události. Požární řád a předpisy BOZP. Případně dokumenty pro řešení mimořádných událostí, jako je živelná katastrofa, havárie nebo požár či výbuch, pokud jsou pro objekt zpracovány.
- Podnikové normativní akty, kam řadíme pokyny, nařízení a směrnice, které upravují práva a povinnosti pro zaměstnance či návštěvníky. Jde o režimová opatření jako kontrola zavazadel na vrátnici, prokázání totožnosti, kontrola vozidla, osobní prohlídka.

1.2 Rozsah bezpečnostní analýzy a následných prací

Zadavatel BA si musí na začátku ujasnit, co požaduje a určit rozsah požadované analýzy. Zda půjde o komplexní zpracování pokrývající všechny prvky, které se na bezpečnosti podílejí, či o dílčí analýzu se zaměřením na jím definované oblasti bezpečnosti. V rámci tohoto rozhodování bychom měli zadavatele vždy poučit o základních faktech a předat mu

stručný nástin problematiky, aby byl schopen učinit samostatné rozhodnutí. Ze zadání objednatele totiž pro analýzu vyplývá rozsah, náročnost, časová náročnost a cena.

1.2.1 Samotná bezpečnostní analýza

- Analýza současného stavu ochrany objektu a bezpečnostních zájmů podniku
- Klady a zápory současného stavu ochrany
- Návrh optimalizace – návrh na zvládání rizik

1.2.2 Doplnění bezpečnostní analýzy

Dle dohody s klientem můžeme samotnou BA obohatit o:

- Bezpečnostní prognózu (odhad vývoje bezpečnostní problematiky ve firmě)
- Bezpečnostní plán (konkrétní projekt ochranných opatření)
- Dokumentace ochrany (směrnice, řád, případně jiné normativní akty)

2 OBSAH BEZPEČNOSTNÍ ANALÝZY

Bezpečnostní analýza má určitou posloupnost procedur. Skládá se z několika základních kroků. Nejprve začínáme studií, kde rámcově definujeme její formu a obsah. Pokračujeme analýzou rizik, kde přistupujeme ke shromažďování informací a dokumetů o zkoumaném objektu a jejich analýze. Následuje vyhodnocení rizik a nakonec návrh zlepšení, tedy optimalizace stavu. Některá literatura, především vinou překladu z angličtiny tuto kompozici mění, někdy je vynechávána část optimalizace. Vinou rozdílnosti překladů také některá literatura směsuje či zaměňuje pojmy hrozba a riziko, a tím dochází v praxi, někdy i mezi odborníky, k rozporům či neporozumění. V následujícím textu jsem tyto pojmy, včetně jejich anglických reprezentací, jasně definoval, aby k neporozumění nedošlo.

Nejprve však musíme vyřešit otázku zpracovatele analýzy, jelikož normy, ani odborná literatura tuto otázku příliš neřeší, přestože jde o velmi podstatné rozhodnutí. Na výběr máme dvě možnosti, buď si analýzu provést sami (interní) nebo najmout firmu (externí), která poskytuje analytickou činnost jako službu. Každý z těchto případů má svá „pro a proti“. Shrneme si je v Tabulka 1. Výběr řešitele bude vždy záviset na konkrétní situaci a prioritách firmy. Někdy může být prioritní zachování důvěry, jindy firma toto hledisko nebude brát jako podstatné a bude vyžadovat raději kvalitní práci, provedenou profesionály s analytickou praxí.

Interní analýza	Externí analýza
Znalost prostředí a procesů	Zkušenosti z jiných analýz objektů
Zachování důvěrnosti	Porušení důvěrnosti
Nutnost koupit nebo vyvinout metodiku	Není nutnost koupit nebo vyvinout metodiku
Nutnost koupit nebo vyvinout nástroj	Není nutnost koupit nebo vyvinout nástroj
Nutnost vlastnit či vyškolit odborníky	Není nutnost mít vlastní odborníky
Nižší míra objektivity (provozní slepota)	Vyšší míra objektivity
Nižší cena	Vyšší cena
Větší časová zátěž pro společnost	Menší časová zátěž pro společnost

Tabulka 1 Klady a zápory interní a externí analýzy

Zdroj 3

Samozřejmě lze také použít v praxi oblíbený kombinovaný přístup, který potlačuje nedostatky dvou předešlých. Znamená to určit jako zpracovatele vlastní zaměstnance, ale nalézt zároveň odbornou firmu, která bude na proces dohlížet a řídit jej. Takto jsme schopni vyškolit si ve firmě vlastní odborníky, kteří budou další analýzy schopni provádět již bez asistence. To je značná výhoda, jelikož analýzu se doporučuje provádět, krom známých situací, zhruba jednou ročně.

2.1 Oblasti rizik

Nyní si uvedeme oblasti, kterých by se komplexní analýza měla týkat. Opět z bezpečnostní politiky vyplývá, které z nich budeme řešit a které vynecháme. Některé oblasti mohou být obligatorní ze zákona, jiné se v naší firmě vůbec nemusejí vyskytovat, kompletní výčet je však následující:

2.1.1 Technologická rizika

Neboli havárie. Tuto oblast řeší metody analýzy jako HAZOP, CPQRA, apod. Jde zejména o výbuch, požár, únik škodlivin ohrožujících zdraví, životy a životní prostředí. Mezi jejich zdroje řadíme mechanicky pohyblivé části, zdroje a úložná místa energií, EM a radiační záření, hluk a vibrace, biologická rizika, lidské selhání na rozhraní člověk – stroj, které ústí v chemické, jaderné a ekologické havárie, softwarové chyby a selhání.

2.1.2 Enviromentální rizika

Lze je zařadit do již zmíněných technologických, jde totiž především o úniky škodlivin. Dnes je tato oblast pro firmy aktuální, jelikož průmyslové havárie v minulosti a jejich následky, jsou odstrašujícím příkladem toho, co se stane, když jsou tato rizika opomíjena. Nesmíme zapomínat jen na škody finanční či lidské, které utrpí náš podnik, ale musíme pamatovat i na možné dlouholeté znehodnocení okolního prostředí podniku. Proto je zde odděluji od technologikých. Zároveň je dnes moderní do bezpečnostní politiky zařadit postup nakládání s odpady, včetně těch běžných (třídění), což zvyšuje prestiž firmy.

2.1.3 Přírodní katastrofy

Nesmíme opomenout ani vnější vlivy na podnik. V našich podmínkách sem patří blizard (sněhová bouře), bouřka, krupobití, horko, sucho, tornádo, zima, sesuv, sopečná erupce, lavina, zemětřesení, epidemie, pandemie, epityfie, povodeň a požár.

2.1.4 Rizika způsobená člověkem

Patří sem katastrofy způsobené lidskou chybou nebo úmyslem. Tedy dopravní nehody, letecké nehody, terorismus, válka, žhářství, výpadek energie, sabotáž - poškození aktiv, vloupání.

2.1.5 Právní rizika

V této oblasti se proti rizikům bráníme především prevencí. Zde totiž i při úspěšném ukončení právního sporu tratíme čas, nervy, pověst, příležitosti, někdy i peníze. Nejzávažnější právní rizika vznikají při:

- Postupu v rozporu se zákonem při právních úkonech souvisejících s existencí organizace.
- Nevhodných interních právních normách.
- Nevhodných smlouvách s dodavateli, odběrateli, zaměstnanci.
- Neošetření ochrany duševního vlastnictví a obchodního tajemství.
- Neošetření ochrany osobních údajů.
- Nedostatečné ochraně majetku, zdraví a života, tedy nedostatečném pojištění.
- Porušování obecně závazných právních předpisů či zvláštních právních předpisů.

Vidíme tedy, že tato rizika jsou velmi závažná, jelikož nejen požár, ale i špatně sepsaná smlouva může znamenat krach. Tuto oblast řeší právní oddělení podniku. Z praxe je nejčastější příčinou problémů v této oblasti neznalost, nedbalost a úmysl.

2.1.6 Informační rizika

Týkají se nejen práce s utajovanými informacemi (dále jen UI). Ze zákona o UI vyplývá, že se jedná o informace, které by mohly při jejich zneužití způsobit újmu zájmům ČR nebo jiným subjektům, s nimiž má ČR smlouvy. I když se ale nejedná o takovýto státní podnik,

může v něm fungovat systém ochrany informací, firmy si dnes střeží svá obchodní tajemství a know how, skladují osobní informace, jejichž ochranu jim ukládá zákon, a proto jsou aplikována opatření i v těchto institucích. Informační riziko bude nejen únik, ale i ztráta či poškození dat v případě, že jsme firmou vyvíjející software nebo skladující data. Informační bezpečnost zajišťujeme například softwarově šifrováním, ale i přísnými pravidly pro přístup k informacím na základě hesel apod. Pro testování informační bezpečnosti organizace slouží například penetrační testy, metoda CRAMM, ale nesmíme zapomínat ani na fyzickou ochranu dat pomocí MZS, EPS a PZTS.

2.1.7 Investiční rizika

Jako marketingové riziko (vytvoření produktu, který nikdo nechce nebo kterému obchodní zástupci nerozumí a neví, jak ho prodat), strategické riziko (vytvoření produktu, který už nezapadá do obchodní strategie podniku), riziko managementu (ztráta podpory projektu ze strany vedení, vlivem změny zaměření nebo změny osob), rozpočtové riziko (nedodržení rozpočtu, nedosažení zisku). Tato rizika mají na starost marketingové a ekonomické oddělení a měly by je řešit průběžně.

2.1.8 BOZP

Především v oblasti výroby lze předpokládat zvýšené riziko pracovních úrazů, či dokonce ohrožení života. Bezpečnost a ochrana zdraví při práci musí být prováděna pomocí opakovaného školení zaměstnanců. Rizika z nedodržení BOZP jsou finanční postihy a samozřejmě ovlivňují i dobrou pověst podniku. Zákoník práce se k povinnostem zaměstnavatelů vyjadřuje obecně těmito slovy: "Zaměstnavatel je povinen soustavně vyhledávat nebezpečné činitele a procesy pracovního prostředí a pracovních podmínek, zjišťovat jejich příčiny a zdroje. Na základě tohoto zjištění vyhledávat a hodnotit rizika a přijímat opatření k jejich odstranění a provádět taková opatření, aby v důsledku příznivějších pracovních podmínek a úrovně rozhodujících faktorů práce dosud zařazené podle zvláštního právního předpisu jako rizikové mohly být zařazeny do kategorie nižší. K tomu je povinen pravidelně kontrolovat úroveň bezpečnosti a ochrany zdraví při práci, zejména stav výrobních a pracovních prostředků a vybavení pracovišť a úroveň rizikových faktorů pracovních podmínek, a dodržovat metody a způsob zjištění a hodnocení rizikových faktorů podle zvláštního právního předpisu.". Neboli je nutné provádět analýzu rizik v této oblasti pro vyhledání a eliminaci rizik na pracovišti.

Samotný obsah BA je poté následovný:

2.2 Studie

Je první etapou bezpečnostní analýzy a řešíme v ní tyto hlavní aspekty:

- Definice problému – Před započetím řešení jakéhokoliv problému je třeba jej specifikovat. V tomto kroku tedy odpovídáme na otázku, které oblasti bezpečnosti jsou pro nás stěžejní, tyto oblasti jsou vymezeny v kapitole 1.
- Obsahové nároky – řeší rozsah a kvalitu zpracované analýzy. Tato problematika je rozebrána v kapitole 1.2. Podrobněji řeší obsahové nároky kapitola 1.1. V tomto kroku též řešíme výběr metodiky a metody, kterou použijeme, jejich dělení a výčet je obsažen v kapitole 3. Řešíme i přístup k analýze, například dle ČSN ISO/IEC TR 13335 :
  - Základní – neprovádíme analýzu, pouze uplatníme sadu opatření, již osvědčenou v podobném provozu. Není příliš vhodné řešení, jelikož riskujeme opomenutí specifických faktorů a hrozeb působících v našem podniku. Je však výhodné při potřebě okamžitého zabezpečení, kdy soupeříme s časem.
  - Neformální – rychlá operační analýza založená na zkušenosti odborníků. Tento pojem lze ztotožnit s kvalitativní analýzou.
  - Formální – detailní analýza, často za použití matematického aparátu. Častěji nazýváme kvantitativní analýza.
  - Kombinovaný – Na základě orientační analýzy se následně provede i detailní. Jde o proces nejzdlouhavější a finančně nejnáročnější, což je však vykoupeno jeho přínosem.
- Časové nároky – Zde stanovujeme termín dokončení analýzy, musíme si však být vědomi, že potřebný čas na vyhotovení je závislý na zvoleném rozsahu.
- Finanční nároky – souvisí s dvěma předchozími aspekty a jsou na nich přímo závislé.
- Nároky na zpracovatelský tým – důležité je také určit kdo bude analýzu provádět, jelikož jde o podstatný výběr s vlivem na průběh a kvalitu celé analýzy. Obvykle máme dvě hlavní skupiny a to vlastníci a expertní tým složený z odborníků na

řešenou oblast analýzy (jiné odborníky vyžadujeme u chemického provozu, jiné u IT firmy, apod.).

2.3 Analýza rizik

Obrázek 1 Průběh AR

Zdroj 19

Druhou etapou BA je identifikace rizik. Laicky řečeno zde zkoumáme co všechno, z jakého důvodu, jakým způsobem a kde se může stát a kdo tím bude dotčen. V této proceduře definujeme hrozby, pravděpodobnost s jakou nastanou a jejich dopad na aktiva. Pro nalezení odpovědí na tyto otázky je analýza rizik rozčleněna na jednotlivé fáze. Pro porozumnění pojmům, jež jsou v analýze rizik používány, je nutné tyto přesně vymezit:

2.3.1 Hrozba (Threat)

Hrozbou rozumíme sílu, událost, aktivitu nebo osobu, jenž je schopna způsobit škodu. Hrozbou je konkrétně požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neoprávněnou osobou, chyba obsluhy. Hrozba využívá zranitelnost, překoná protiopatření a působí na aktivum, kde vyvolá škodu (dopad). Hrozba zasahuje přímo aktivum nebo jeho protiopatření, za účelem získání kontroly nad aktivem. Pro realizaci hrozby je nutné ji aktivovat – vytvořit podmínky pro její působení. Její základní vlastností je úroveň, kterou hodnotíme především podle nebezpečnosti neboli schopnosti hrozby škodu způsobit, dále dle přístupu, tedy pravděpodobnosti s jakou se hrozba přiblíží k aktivu (lze vyjádřit například frekvencí výskytu) a nakonec dle motivace, tedy zájmu jednotlivců či skupin hrozbu uskutečnit.

2.3.2 Protiopatření (Countermeasure)

Znamená buďto postup, proces, proceduru, technický prostředek či jiné opatření pro minimalizaci působení hrozby, zranitelnosti nebo dopadu. Protiopatření jsou koncipována s cílem předejít vzniku škod nebo usnadnění revitalizace po vzniklé škodě. Protiopatření je charakterizováno efektivitou a náklady, tím rozumíme sumu za pořízení, zavedení a provoz. Efektivitou rozumíme nakolik protiopatření redukuje účinek hrozby a jde o hlavní parametr, podle kterého vybíráme vhodná protiopatření, avšak pro optimalizaci hledáme taková, která mají co nejmenší náklady. Protiopatření ochraňuje aktiva, detekuje hrozby a minimalizuje či eliminuje jejich působení na aktiva. Protiopatření také odrazují od aktivace hrozeb.

2.3.3 Riziko (Risk)

Pravděpodobnost vzniku hrozby, je ji možno vyjádřit procentuálně či stupnicově, přičemž takto hodnotíme základní vlastnost rizika, kterou je jeho úroveň. Tato je snižována pomocí protiopatření a naopak eskaluje s hodnotou aktiva, úrovní hrozby a zranitelnosti. Termín „risico“ pochází původně z italštiny, kde označuje „úskalí“, jemuž museli čelit námořníci. Jde tedy obecně o nebezpečí, že s určitou pravděpodobností vznikne událost, jenž je z bezpečnostního hlediska nežádoucí. Riziko je pokaždé odvoditelné a odvozené z konkrétní hrozby. Jeho míru je možné posoudit na základě analýzy rizik, která ukazuje naši připravenosti vůči hrozbám. Riziko je výsledkem interakce hrozby a aktiva, pokud hrozba neohrožuje žádné aktivum, je z analýzy vynechána.

Při tvorbě protiopatření dbáme na to, aby náklady vynaložené na redukci rizika nepřesáhly hodnotu chráněného aktiva, či škod vzniklých uplatněním hrozby. Stanovujeme určitou ***referenční úroveň***, která je hranicí míry rizika. Pomáhá nám rozhodnout, proti kterým rizikům je nutné podnikat protiopatření, protože ta se v praxi nikdy nedělají na 100 %. Pokud tedy úroveň rizika leží pod tou referenční, označujeme jej jako ***zbytkové riziko*** a protiopatření neprovádíme, jelikož dopad je pro nás zanedbatelný. Rizika můžeme členit na bezprostřední, která jsou okamžitě viditelná, následná neboli sekundární, kdy může dojít k řetězení, kdy dopadem jednoho rizika vzniká nová hrozba. Takto se při nešťastné shodě náhod může naplnit scénář s katastrofickými následky. Posledním typem rizika jsou latentní, tedy skrytá, která nemusíme na první pohled vůbec vidět, pro jejich odhalení

slouží právě analýza rizik. Riziko se obvykle nevyskytuje zcela samostatně, proto určujeme priority jednotlivých rizik, abychom byli schopni následně řešit nejvíce rizikové oblasti.

2.3.4 Aktivum (Asset)

Znamená cokoliv, jenž má pro subjekt určitou hodnotu, která může být redukována vlivem hrozby. Hodnotu aktiva uvádíme buď cenou (u kvantitativní analýzy) nebo odstupňovaně pomocí slov či číslic (1 až 5 nebo nízká, až velmi vysoká). Bereme přitom jako východiska hlavně pořizovací náklady či jinou hodnotu, důležitost pro subjekt, náklady na překonání škody způsobené na aktivu a rychlost tohoto překonání a jiná specifická hlediska. Aktiva rozdělujeme na:
hmotná (například peníze, nemovitosti, cenné papíry, apod.)
nehmotná (například informace, prestiž organizace, morálka pracovníků, kvalita personálu, apod. Tato mohou mít pro nás někdy větší hodnotu než aktiva hmotná, jelikož případná kompromitace nehmotných aktiv může být u některých organizací nevyčíslitelná.). Aktivem lze označit i samotný subjekt, protože hrozba na něj může působit jako na celek. Aktivum svojí základní vlastností – hodnotou, vybízí a motivuje útočníka k naplnění hrozby, hodnotu aktiva zároveň potřebujeme znát do vzorce pro výpočet rizika. Před účinkem hrozby má aktivum jistou zranitelnost, zároveň je také chráněno před hrozbami pomocí protiopatření.

2.3.5 Zranitelnost (Vulnerability)

Znamená slabinu aktiva, která může být zneužita hrozbou, čímž může dojít k naplnění hrozby. Zranitelnost je vlastností aktiva a znamená to, jak citlivé je aktivum na danou hrozbu. Vyskytuje se na místech, kde dochází k interakci mezi aktivem a hrozbou. Z hlediska jejího stupně, hodnotíme podle :

citlivosti - náchylnost aktiva na poškození danou hrozbou
kritičnosti - významnost aktiva pro analyzovaný subjekt.
Míra zranitelnosti je pro nás podstatná hodnota, jelikož ji musíme znát pro výpočet rizika.

2.3.6 Dopad (Consequence)

Jde o míru zasažení aktiva po uskutečnění hrozby. Lze vyjádřit například finančně při aplikaci kvantitativní analýzy jako ztrátu, součtem všech hodnot zasažených aktiv. Lze ho

též vyjádřit v nehmotné rovině jako třeba zneuctění dobrého jména firmy nebo kompromitace know how, což jsou v podstatě nevyčíslitelné položky a přistupujeme zde spíše ke slovnímu hodnocení (např. zanedbatelný až kritický). Obecně je to tedy škoda jakéhokoliv charakteru způsobená realizací hrozby. V praxi můžeme vyjádřit finanční ztráty přímé v poměru ku nepřímým (sekundárním), abychom získali lepší přehled o možných následcích, často totiž sekundární ztráty značně převyšují ty primární (Například porucha vyřadí z provozu PLC automat, čímž ale sekundárně zneschopní celou linku a my tak tratíme na výrobě.).

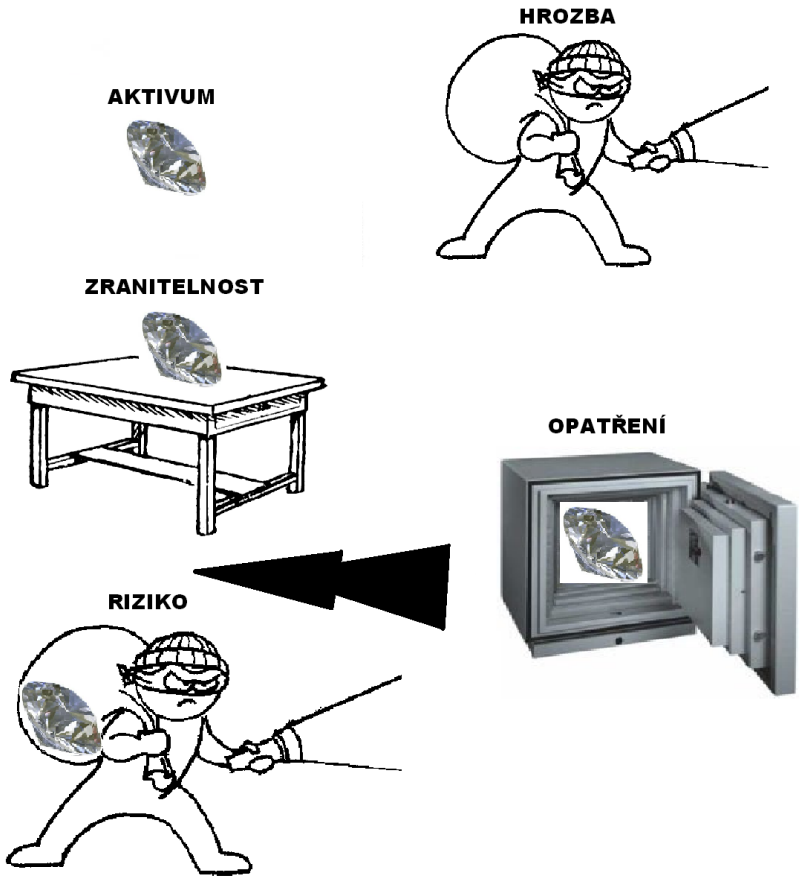
2.3.7 Ohrožení (Exposure)

Tento pojem, stejně jako následující (narušení), není tak často užíván, přesto se v literatuře vyskytuje a je vhodné je zmínit i zde. Jde o fakt, že existuje zranitelnost, která může být zneužita hrozbou. Jde tedy o stav, nikoliv o vyčíslitelnou položku.

2.3.8 Narušení (Breach)

Situace, kdy dojde k narušení důvěrnosti, integrity či dostupnosti aktiv v důsledku překonání bezpečnostních opatření. Opět se jedná o stav, stejně jako předchozí termín.

Dost často dochází ke záměně pojmů riziko a hrozba. Rozdíl je však v tom, že hrozba může být zdrojem pro jedno i více rizik a že hrozba samotná riziko nepředstavuje. Hrozby pouze zneužívají zranitelnosti vedoucí k ohrožení, což je riziko, které lze snížit prostřednictvím opatření chránících aktiva před působením těchto hrozeb. Tento rozdíl nám lépe pomůže pochopit následující Obrázek 2.



Obrázek 2 Vztahy v analýze rizik

Zdroj vlastní

Nyní můžeme popsat objednotlivé fáze AR:

2.3.9 Analýza aktiv

Pro potřeby analýzy musíme nejprve stanovit aktiva (všechny druhy majetku na kterém nám záleží a jehož případné znehodnocení či ztráta jsou pro nás neakceptovatelné). V tomto kroku určí většinou zadavatel analýzy hranici, kterou je specifikováno, která aktiva budou zahrnuta do analýzy a která již ne. Je totiž zřejmé, že poškození zvonku na dveřích firmy či krádež květináče z areálu nejsou většinou aktiva, která by pro nás byla zajímavá a podstatná. Dále aktiva ohodnotíme dle důležitosti, například osobní počítač bude mít jistě pro nás menší hodnotu než stroj, který zajišťuje v našem podniku hlavní podíl produkce (samozřejmě za předpokladu, že na počítači není uloženo know-how naší firmy či jiná kompromitující data). Rozlišujeme tedy, zda je aktivum jedinečné, či snadno nahraditelné. Aktiva hodnotíme dle újmy, která vznikne ztrátou či zničením aktiva. Tato újma může být

nákladová (stanovena dle pořizovací ceny či ceny opravy) nebo výnosová (pokud se jedná o stroj nebo jiný atribut, který firmě tvoří zisk) a také nepřímo výnosová (netvoří zisk přímo, ale jako svůj postranní efekt – know how, ochranná známka). Hodnota újmy se počítá ze ztráty v důsledku omezení funkčnosti, či zneprovoznění aktiva až do jeho obnovy. Podstatné je také rozlišit, zda je aktivum snadno nahraditelné nebo jedinečné. Aktiva je možno pro zjednodušení práce seskupovat. Seskupování se provádí podle společných znaků jako je cena, účel nebo kvalita. Následně bereme každou skupinu aktiv jako jedno jediné aktivum. Ve fázi zvládání rizik poté musíme dohlédnout na aplikaci protiopatření na všechna aktiva ze skupiny.

2.3.10 Analýza hrozeb

Dále identifikujeme a oceňujeme hrozby, tedy situace, které budou mít negativní dopad na důvěrnost, integritu či dostupnost aktiv. Každý systém může být ohrožován určitými hrozbami a proto abychom jim dokázali účelně čelit, musíme je nejprve správně identifikovat. Hrozby sestavujeme z již hotových seznamů v literatuře, vlastních odhadů či minulých analýz, můžeme také porovnat hrozby v podobném systému. Budeme se přitom soustředit na toky energií v objektu, nebezpečné materiály, interakci prvků systému (například chemikálie), rozhranní člověk – stroj, apod. Vybíráme vždy takové hrozby, jež jsou svým charakterem schopny ohrozit minimálně jedno aktivum. Také definujeme pravděpodobnost výskytu hrozby. Při tomto hodnocení je nutné zaměřit se na klíčová riziková místa a správně určit priority dopadu a pravděpodobnosti hrozeb. Každou hrozbu hodnotíme vzhledem ke každému aktivu či skupině aktiv. U aktiv, která mohou být hrozbou zasažena pak určíme úroveň hrozby (kdy hodnotíme nebezpečnost, motivaci a přístup k aktivu). Při prvním kroku identifikace hrozeb je vhodné tyto kategorizovat, existují mnohá členění, nejčastější z nich jsou podle úmyslu a lokace zdroje:

Dle úmyslu členíme na:

- Náhodné – zde řadíme zcela náhodné hrozby, jejichž původ je v literatuře znám jako threat event.
- Úmyslné – sem řadíme hrozby, jež byly plánované, původce se označuje jako threat agent.

Dle lokace zdroje:

- Vnitřní – neboli interní, jejichž zdroj je umístěn uvnitř systému.
- Vnější - neboli externí, jejichž zdroj je umístěn vně systému.

Zkombinováním předešlých členění můžeme utvořit Matice hrozeb, která reprezentuje 4 základní typy hrozeb, do těchto čtyř kategorií lze začlenit prakticky jakoukoliv hrozbu:

	náhodné	**úmyslné**
externí	přírodního původu	činnost kriminálních živlů
interní	technické selhání a lidská chyba	sabotáž

Tabulka 2 Matice hrozeb

Zdroj 19

U firem zabývajících se IT lze použít i členění z hlediska dopadu na systém. Toto se v praxi příliš nepoužívá, ale jeho přínosem je identifikace, kterou ze složek bezpečnosti (integrita, důvěrnost, dostupnost) hrozba ohrožuje. Dělíme na:

- Aktivní – kdy dojde ke změně stavu systému kvůli narušení integrity a dostupnosti
- Pasivní – nedochází ke změně stavu, „pouze“ k úniku informací

Pro proces analýzy má toto členění význam pouze jako pomůcka při identifikaci hrozeb. Většího významu dosáhne při ocenění rizik, kdy nám dává přehled o tom, jaké hrozby jsou pro systém stěžejní. Hrozby následně seskupujeme většinou podle aktiva, na které působí, jelikož poté při rozhodování, zda je daná hrozba relevantní pro určité aktivum (jelikož ne každé aktivum je ohroženo všemi hrozbami), již nemarníme čas.

2.3.11 Analýza zranitelnosti

Při určování míry zranitelnosti postupně procházíme všechny dvojice hrozba-aktivum a přiřazujeme jim hodnoty zranitelnosti. Tuto míru hodnotíme především na základě citlivosti a kritičnosti. V úvahu bereme i zavedená protiopatření, která samozřejmě zranitelnost snižují, proto výsledná škoda bývá menší, než celková hodnota aktiva. Výsledek této analýzy je seznam dvojic hrozba-aktivum s příslušnou mírou rizika. V případě kvantitativní analýzy tuto míru uvádíme obvykle v procentech. U kvalitativního postupu stanovíme několik úrovní zranitelnosti, obvykle tři až čtyři. Lze použít následující

Tabulka 3, ale počet úrovní v praxi vždy přizpůsobujeme konkrétní situaci, tabulka tedy není dogmatem.

úroveň	***popis***
kritická	Neexistují žádná protiopatření
vysoká	Opatření existují, ale předpokládáme jejich selhání
střední	Opatření existují, předpokládáme jejich účinnost
nízká	Jsme přesvědčeni o spolehlivosti opatření

Tabulka 3 Příklad úrovní zranitelnosti pro kvalitativní analýzu

Zdroj 19

Při hodnocení pravděpodobnosti jevu jev nastává buďto zcela náhodně nebo je ho možné předpovědět, jelikož nastává za podmínek podmíněné pravděpodobnosti neboli pravděpodobnost výskytu jevu je podmíněna výskytem jiného jevu. Zde se uplatní matematická statistika. Při výpočtu rizika pracujeme s hodnotami, které velmi často není možné změřit a proto na řadu přichází kvalifikovaný odhad, jehož výstupem je obvykle odstupňování (malý, střední, velký) nebo číselné vyjádření 1 až 10 apod.

2.3.12 Stanovení výše rizika nebo škody

V této fázi přicházíme k hodnocení případných škod. V praxi můžeme opět použít stupnicový systém, tedy v případě kvalitativní analýzy, kdy škodu vyjadřujeme obvykle slovně v rozmezí od banální, přes střední až po fatální, která by znamenala ukončení provozu podniku, jako třeba destrukce hlavního výrobního stroje či podobně. Někdy je však výhodnější škodu přímo vyčíslit, tedy použijeme kvantitativní analýzu, abychom znali hodnotu ztráty a dokázali se na ni připravit, například formou pojištění. Kompromisem je kombinovaný přístup k analýze, kdy dopad rizik pomocí kvantitativní analýzy vyčíslíme finančně a zároveň pomocí kvalitativní analýzy jednotlivá rizika zařadíme do slovně hodnocených kategorií, která jasně vyjadřují jejich důsledek pro firmu. Pro rizika v kategorii fatální je vhodné zpracovat havarijní, či obdobný plán.

Výpočet rizika se bude mírně lišit pokud provádíme analýzu kvalitativně nebo kvantitativně, jak je rozebráno v příslušných kapitolách. Základními prvky rovnic budou hodnota aktiva, pravděpodobnost hrozby a míra zranitelnosti.

2.4 Vyhodnocení rizik

Některé rizikové analýzy již tento krok obsahují, v případech, kdy je tomu naopak zahajujeme jej v této fázi. Jde o stanovení rizik, která vyšla z analýzy rizik jako kritická, či jsou pro nás jiným způsobem podstatná a hodláme se jimi zabývat v další fázi analýzy. Při vyhodnocování, zda je riziko tolerovatelné lze vycházet z následující matice:

Pravděpodobnost vzniku havárie	**Úroveň dopadu havárie**		
	nepatrná	**významná**	**značná**
velmi nepravděpodobná	**bezvýznamné riziko**	nízké riziko	střední riziko
nepravděpodobná	nízké riziko	střední riziko	**značné riziko**
pravděpodobná	střední riziko	**značné riziko**	**netolerovatelné riziko**

Tabulka 4 Matice rizik

Zdroj 15

2.5 Návrh zlepšení

V tomto kroku na základě připravenosti a funkčnosti zavedených protiopatření navrhujeme, jak je inovovat, abychom dosáhli maximální účinnosti opět za vynaložení minimálních prostředků. Těmito inovacemi se snažíme dosáhnout cílového stavu zabezpečení, který vyplývá z bezpečnostní politiky. Navrhujeme zde bezpečnostní mechanismy a opatření, kterými rizika snižujeme. Zároveň lze zpracovat inovovaný návrh zásad bezpečnostní politiky, který pak do politiky podniku promítneme, analýza tedy zároveň poskytuje zpětnou vazbu. Nejedná se o plán zabezpečení, jak by si mohl někdo myslet, jde pouze o jakousi jeho předběžnou verzi, kde ještě nespecifikujeme zcela konkrétně, jak přesně ochranu vylepšit. Tento návrh tvoří pouze koncepční souhrn rad a doporučení, která by měl následný plán respektovat, jelikož právě za tímto účelem je celá předchozí práce prováděna (např. navrhneme pouze použití kamerového systému a umístění kamer, ne však konkrétní typ). Ať už se jedná o PZTS, EPS, režimová opatření, nedostatky v bezpečnosti výroby či nespolehlivost lidských zdrojů, vždy lze něco zlepšit. Opět však musíme optimálně určit jaká vylepšení pro nás budou dostatečně přínosná. Nemá cenu investovat do přehnaných opatření, která ve výsledku budou mít jen malý podíl na zvýšení úrovně bezpečnosti. Je to

opět závislé na prioritách firmy, například solidní podnik zajišťující úschovu počítačových dat by měl mít nepochybně samohasící systém, který v případě požáru okamžitě neutralizuje jeho působení. Vychází to z charakteru chráněného zájmu, v tomto případě dat, která mají pro zákazníky firmy nedozírnou hodnotu. V tomto případě prostě nestačí běžné senzory a následný výjezd hasičů, kdy nám případné škody pokryje pojišťovna jako by to bylo dostačující u běžného výrobního provozu.

V tomto kroku tedy rozhodujeme o nakládání s riziky. Můžeme volit mezi taktikou defenzivní a ofenzivní. Ofenzivní opatření jsou přímá, která eliminují zdroje rizika, lze je však použít pouze tehdy, pokud má firma možnost tyto zdroje ovlivnit. Defenzivní opatření jsou vhodná spíše k potlačení neblahých následků a jejich zmírnění, typickým zástupcem je pojištění. Dle zařazení rizika do jedné z následujících kategorií stanovíme způsob, jak s ním nakládat. Existují tyto základní postupy:

- přenesení na jiné subjekty (transfer) – Jde o typicky defenzivní přístup, kdy se zbavujeme odpovědnosti za možné riziko. V našem oboru se bude typicky jednat o smluvní vztah s hlídací agenturou, které platíme za bezproblémový stav bezpečnostní situace v naší firmě. Lze sem jednoznačně zařadit i pojištění.

- pojištění – Je vhodné použít především u rizik s malou pravděpodobností nebo zcela nahodilým, obtížně ovlivnitelným výskytem a zároveň s vysokým rizikem, existenčně ohrožujícím náš podnik. Při vysoké pravděpodobnosti rizikového stavu by pojištění bylo již příliš nákladné. V praxi je vhodné pojistit podnik proti požáru, případně krádeži, pokud máme v objektu EZS a EPS systémy, zredukuje to výši pojistného a zároveň jsme chráněni finančním krytím proti selhání těchto systémů.

- rozklad – Neboli diverzifikace rizika, kdy rozdělujeme odpovědnost za riziko mezi více subjektů.

- ignorování rizika – Na riziko nereagujeme protiopatřeními nebo dokonce úplně vynecháme stávající opatření. Riziko je tedy neřízeno. Používá se výhradně pro rizika s malou četností a malou škodou. Přestože se tato forma nakládání s riziky může jevit jako amatérská a nezodpovědná, není tomu tak. Jde o zcela legitimní metodu, kterou využijeme právě v případech, kdy stupeň daného rizika leží pod referenční úrovní rizika. Někdy se setkáváme s pojmem retence neboli zadržení rizik.

- sledování rizika – Jde o monitorování výskytu rizikových událostí a hodnot rizikových faktorů. Opatření nasadíme až v případě zvýšeného výskytu rizika nebo alarmujících hodnot rizikových faktorů. V našem případě se jedná například o CCTV, pomocí kterého obsluha sleduje střežený zájem a až po narušení jeho bezpečnosti podnikne odpovídající kroky jako přivolání pomoci nebo přímý zásah.

- prevence rizika – Tím rozumíme předcházení vzniku rizikových událostí za pomoci opatření redukujících četnost vzniku rizika pomocí snižování hodnot rizikových faktorů. V našem případě sem můžeme zařadit MZS nebo ACCESS, které brání přístupu neoprávněných osob.

- redukce rizika – Jedná se o obdobu prevence. Rizikové události potlačujeme represivními opatřeními u rizik s vysokou četností. Taková minimalizace v praxi bude znamenat obecně zavedení bezpečnostních opatření.

- eliminace – Jde o úplné zrušení činností nebo zdrojů, které představují rizikové faktory. Používá se pro rizika s vysokou škodou i pravděpodobností. Pokud nelze roziko zcela eliminovat, přistupujeme k redukci.

Po návrhu jak s identifikovanými riziky pracovat se tyto skutečnosti zpětně promítají do bezpečnostní politiky.

AR je asi nejdůležitějším článkem řetězce v bezpečnostní analýze, ale musíme brát na zřetel fakt, že vše co z ní vyplyne, je pouhý odhad nebo přibližný výsledek. To je dáno dvěma hlavními důvody. Za prvé, obvykle zkoumáme model systému a nikoliv systém samotný. Za druhé, při prognózování vycházíme z názorů respondentů. Jeden zpracovatel pojmutí všech potřebných informací reálně nezvládá a je odkázán na osoby, které mu ne vždy poskytnou všechny potřebné podklady. Paradoxně se navíc v praxi ukázalo, že při pronikání k podrobnějším detailům o systému se vzdalujeme od možnosti podchytit všechny souvislosti.

3 METODIKA ANALÝZY

Pro většinu následujících typů analýz platí termíny z předchozí kapitoly. Je nutné však říci, že neexistuje žádná univerzální metoda, naopak každá metoda je trochu odlišná, a proto více či méně vhodná pro konkrétní aplikaci, záleží již na analytikovi a jeho zkušenostech, jakou metodu pro konkrétní situaci zvolí. Při výběru metodiky analýzy vycházíme z cílů (nároky na přesnost výstupu a nároků bezpečnostní politiky), pro které bude analýza sloužit, dále z kvality vstupních údajů, ze zdrojů rizika a také z požadavků a předpokladů konkrétní metodiky. Je dobré si uvědomit, že všechny analytické metody jsou pouze pomocnými nástroji, kdy hlavní práci tvoří lidská inteligence, bez které by proces nemohl odpovídajícím způsobem fungovat.

Při analýze rizik je možné a také vhodné použít specializovaný software, což nám urychlí práci a umožní operativně měnit parametry. Tyto programové mástroje jsou obvykle specializovány pro konkrétní metodu (ETA, CRAMM, FMEA,…). Jedním z takových nástrojů je například rizikový kalkulátor pro kvalitativní analýzu Riskan nebo nástroj pro výpočet zasažené plochy při úniku nebezpečné látky či výbuchu TerEx. Je samozřejmě možné použít i standartní software (například OFFICE) či dokonce běžný papír. To ale přichází ke slovu spíše v případě nutnosti provedení rychlé operativní analýzy za nedostatku času nebo pokud provádíme analýzu jednoduššího objektu.

Pro analýzu existují dvě základní kategorie (metodiky), kvantitativní a kvalitativní, do kterých pak spadají již konkrétní metody řešení analýzy. Je nutné si uvědomit, že neexistuje jeden univerzální způsob aplikovatelný kdykoliv. Vždy je potřeba zvážit kvalitu vstupních údajů a podle té zvolit jednu ze dvou základních kategorií z níž je pak nutné vybrat adekvátní metodu, opět dle okolností. U chemických provozů se nejčastěji používají metody indexové, kdy pracujeme s pravděpodobností hrozby a výší škody, tím získáme seznam priorit jednotlivých rizik, přičemž ta nejzávažnější dále analyzujeme. Pro rychlý přehled je zde Tabulka 5, vyjadřující klady a zápory těchto dvou metodik.

	Kvantitativní	**Kvalitativní**
náročnost výpočtu	-	+
výsledek	+ transparentní	- diskutabilní
celková cena	-	+

náročnost na programové vybavení	-	+
náročnost na lidské zdroje	-	+
časová náročnost	-	+
kontrola nákladů	+	-
přesnost	+	-

Tabulka 5 Porovnání metodik

Zdroj 19

Bylo by však nemoudré odsoudit kvůli většímu počtu mínusů metodiku kvantitativní. Obě mají svá specifika a v konkrétních případech se může více hodit ta či ona. Většinou u rozsáhlých systémů či objektů k rychlému zhodnocení největších rizik přistupujeme kvalitativně a poté, pokud je třeba je vyčíslit v penězích, pokračujeme kvantitativně se zaměřením pouze na hlavní rizika, která nám vyplynula z předchozí kvalitativní analýzy.

3.1 Kvantitativní metody

Jsou exaktní metody, které jsou náročné na zdroje i časově, používáme formalizované vstupy a matematické výpočty rizika odvozené z frekvence výskytu hrozeb a jejich dopadů, obvykle použijeme finanční vyjádření, například předpokládanou roční ztrátu. Trvá tedy mnohem déle než kvalitativní, avšak na druhou stranu nám přináší kompletní přehled celé bezpečnostní situace a především po výpočtu ztrát v penězích nám umožňuje jednodušší rozhodování. Vyčíslení škody má největší sílu v možnosti porovnání výše škody a ceny protiopatření, tedy jasně si dokážeme spočíst, zda vynaložené prostředky na protiopatření budou efektivně zhodnoceny a nebudou naopak dražší než případná škoda. To u stupňového hodnocení není možné. V prvním kroku identifikujeme a kvantifikujeme aktiva. Ve druhém kroku hrozby. Ve třetím určujeme zranitelnost a poté vyjádříme součinem tří předešlých veličin ztrátu. Důraz je kladen na dostupnost a spolehlivost vstupních dat, při jejich nedostatku či nejednoznačnosti musíme přistoupit ke kvalitativní analýze. Tento typ analýzy obvykle využívá speciálně vyvinuté programové nástroje. Ty obsahují databázované informace a mají v sobě obsaženu metodu pro tvorbu příslušné analýzy.

Metody kvantitavní analýzy jsou následující:

3.1.1 Analýza souvztažností

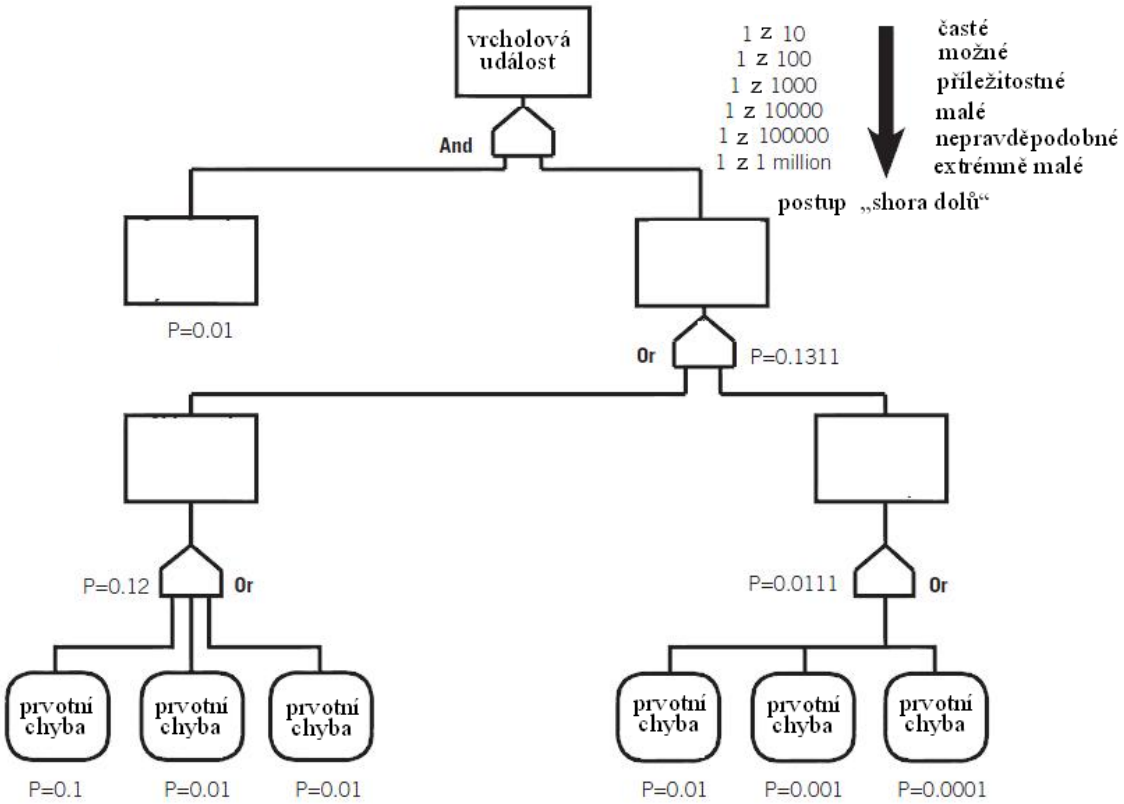
Jde o jednu z metod používaných při analýze objektů bezpečnostními agenturami. Při její aplikaci se doporučuje provést analýzu pro každý objekt (budovu) podniku zvlášť. Analýza je především zaměřena na hledání a hodnocení souvztažností neboli vazeb jednotlivých prvků systému. Nevýhodou této metody je velká pracnost, jelikož vyžaduje detailní zmapování podniku v oblastech materiálů, personálu, postupů a procesů. Tato nevýhoda je vyvážena komplexním přehledem o bezpečnostní situaci podniku. Probíhá ve třech etapách:

- I etapa – identifikace hrozeb, při této činnosti se nejlépe osvědčily statistické analýzy mimořádných událostí za posledních 3 až 5 let. K těmto hrozbám přiřazujeme přímé ztráty na obnovu poškozených aktiv.
- II etapa – zde stanovujeme dílčí pojmy a metody analýzy, obvykle k jednotlivým pojmům provádíme příslušný druh analýzy, tedy pro čas je to průlomová analýza, pro pravděpodobnost analýza druhu rizik, pro přímé následky kvalitativní analýza, pro nepřímé následky (latentní) analýza souvztažností a pro spolehlivost lidských zdrojů analýza pomocí osobnostních psychotestů. V této fázi také definujeme vzorec pro výpočet rizika, někdy se setkáváme se vzorcem R=N*P neboli riziko je následek krát pravděpodobnost.
- III etapa – v nejsložitější etapě oceníme jednotlivé hrozby, rizika a krizové situace z hlediska časové posloupnosti, pravděpodobnosti a jejich vzájemných vazeb. Cílem této etapy je kvalifikovat a finančně zhodnotit rizika.

3.1.2 Fault Tree Analysis (FTA) – Analýza stromem poruch

Základ metody je zpětný rozbor událostí vedoucích ke zkoumané události. Jde o metodu graficko-analytickou či graficko-statistickou. Samotné zobrazení stromu poruch je pak formou rozvětveného grafu s dohodnutými symboly a popisem. Cílem této analýzy je určit pravděpodobnost výskytu zkoumané události za použití analytických nebo statistických metod. Vytváříme různé kombinace poruch a lidských selhání, jež mohou vyústit ve zkoumanou událost na vrcholu stromu. Metoda FTA byla vyvinuta v roce 1960 a je nejčastější metodou pro kvantitativní hodnocení rizik. FTA je deduktivní technika, zkoumající jednotlivou mimořádnou událost v systému a dává nám návod pro odhalení příčin této události. Tím se odlišuje od FMEA, která je technikou induktivní „zdola

nahoru“. FTA znamená postup „shora dolů“, analýza tedy začíná mimořádnou událostí (vrcholová událost - na vrcholu stromu) a zkoumáme bezprostřední příčiny této události. Výstupem je „strom poruch“ propojen pomocí zákonitostí a symbolů booleovy algebry, který ukazuje vztahy mezi primárními událostmi ve spodní části a zvolenou vrcholovou událostí. FTA je technikou deduktivní a následnou indukcí vyslovujeme předběžnou hypotézu, která je přijatelná, pokud dostatečně uspokojivě vysvětluje fakt který zkoumáme. Principem dedukce posléze testujeme tuto hypotézu, jestli má obecnou platnost. Popis metody je zpracován mimo jiné v normě ČSN EN 61025 - Analýza stromu poruchových stavů. Obrázek 3 nám ukazuje příklad takového stromu, na jeho vrcholu je subsystém, v praxi je totiž jednodušší rozdělit si systém na podsystémy a pro každý zpracovat strom poruch, následně jsme pak schopni sestavit i celkový strom systému, kde jsou jednotlivými poruchami již nefunkčnosti celých podsystémů. Graf se tak zjednoduší. FTA je výborným nástrojem ke zjištění odolnosti systému vůči jednotlivým prvotním chybám, nehodí se však už k nalezení všech možných prvotních chyb.



Obrázek 3 FTA

Zdroj 23

3.1.3 Failure Mode and Effect Analysis (FMEA) – Analýza selhání a jejich dopadů

Někdy se používá překlad „analýza příčin poruch a jejich důsledků“. Je jedním z prvních systematických postupů analýzy selhání, který se používal už od 50. let minulého století v USA. Je metodou identifikující vznik případných vad ve výrobním procesu a jejich následků. Pomocí této metody lze detekovat rizika už v ranné fázi výrobního procesu, tedy ještě před zahájením výroby a tím lze dosáhnout maximální úspory prostředků. Výrobní proces je tím pádem také podrobně rozpracován a zdokumentován. Nejdůležitějším přínosem metody ja však samozřejmě identifikace kroků k zamezení vzniku vad či jejich omezení. Principem metody je rozbor způsobů selhání a jejich důsledků, což umožňuje odhalení dopadů a příčin na základě určených selhání zařízení. Své využití nalézá hlavně u vážných rizik. Požadavky na metodu jsou výkonná počítačová technika, speciální výpočetní program, náročná a cíleně zaměřená databáze.

Pro praktické použití metody slouží norma ČSN EN 60812 . Rovněž je vyvinut softwarový nástroj, který je využitelný zejména pro větší korporace, u malých a středních firem si obvykle vystačíme s programy balíku office (excel,word). Jedná se totiž o jednoduchou tabulku, do které vkládáme data získáná například brainstormingem. Typický příklad záhlaví takové tabulky vidíme na následující Tabulka 6.

Prvek	Porucha	Příčina	Detekce	Následek	Doporučení

Tabulka 6 Záhlaví FMEA

Zdroj 14

Brainstormingem odhalujeme všechny možné vady v procesu a zároveň jim přiřazujeme možné následky a příčiny.

FMEA je týmovou metodou, jelikož je zde nutná spolupráce s odborníky znalými vyrobního procesu z různých úrovní řízení. Pro každého takového odborníka je totiž důležitá jiná část výroby a tak se ve výsledku dopátráme k maximálnímu možnému počtu vad, na rozdíl od situace když by analýzu zpracovával jedinec. Prakticky se metoda skládá z osmi hlavních procedur (sestavit realizační tým, vyspecifikovat všechny možné nebo pravděpodobné vady návrhu, stanovení priorit, rozdělení do kategorií, hodnocení, navržení příslušných opatření, provedení opatření, vyhodnocení nového stavu). Výsledkem hodnocení jsou obvykle číselné hodnoty, odrážející nebezpečnost dané události. Je zřejmé,

že u událostí s vyšším číslem na ně musíme zaměřit maximum své pozornosti. Avšak v určitých případech se mohou vyskytnout i události s nízkým číslem dopadu, a přesto je jejich řešení pro organizaci z nějakého důvodu podstatné, to je již odvislé od konkrétních postojů organizace. FMEA je výbornou metodou k získání vyčerpávajícího výčtu prvotních chyb, není však vhodná ke zkoumání vícečetných chyb či jejich efektů na určitou úroveň systému. Metoda je finančně i časově značně náročná, ovšem po zpracování je hodnotným základem například pro další analýzy jako FTA nebo ETA. Při tvorbě této analýzy hledáme odpovědi na tyto otázky:

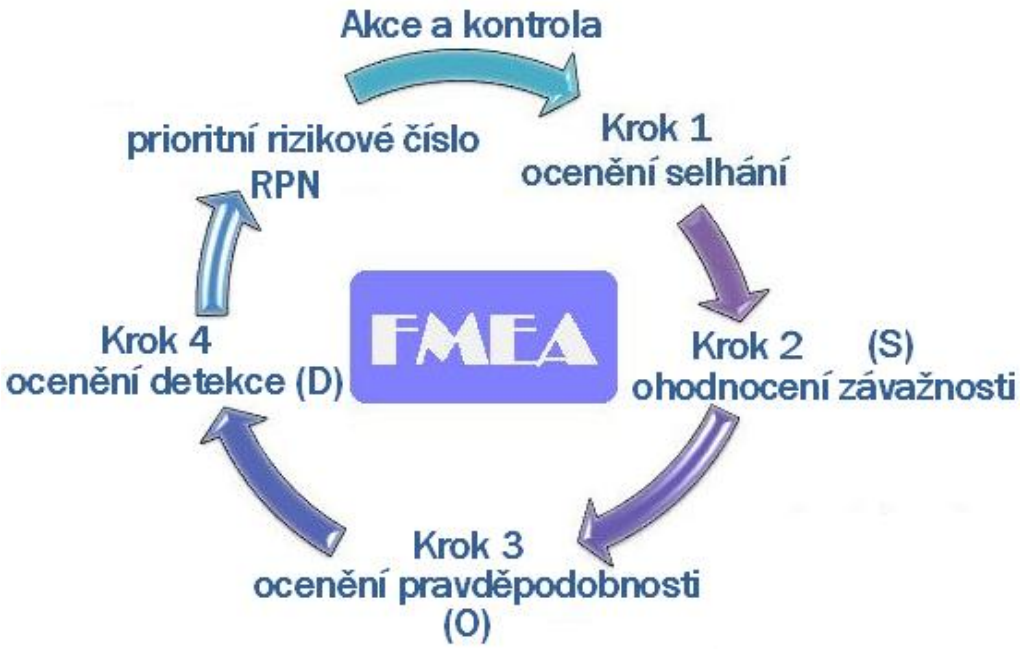
- Jakým způsobem může určitý kompoment selhat?
- Co může toto selhání vyvolat?
- Jaké jsou možné efekty, pokud dojde k selhání?
- Jak významná jsou tato selhání?
- Jakým způsobem detekujeme jednotlivá selhání?

FMEA probíhá ve třech fázích:

- Analýza a hodnocení současného stavu
- Návrh opatření
- Hodnocení stavu po realizaci opatření

Postup první fáze je znázorněn na Obrázek 4. V prvním kroku identifikujeme jednotlivá selhání. Selháním rozumíme všechna vybočení v procesu, na výrobku, a podobně, jež budou mít negativní efekt na zákazníka. Zároveň mohou být aktuální nebo potenciální.

Ve druhém kroku hodnotíme závažnost selhání (S - severity). Jde v podstatě o následek určitého selhání, lze použít různé rozsahy stupnice. Krok 3 oceňuje pravděpodobnost výskytu selhání (O - occurrence). Jako poslední hodnocení přiřazujeme hodnoty k detekci (D - detection) selhání, tato hodnota se někdy vypouští a je pak samozřejmě vynechána i ze vzorce pro výpočet RPN. Poté přistupujeme k výpočtu rizikového čísla (RPN – risk priority number), které získáme jednoduchým vynásobením předešlých veličin $RPN = S * O * D$. Výsledné RPN číslo pak hraje důležitou roli v rozhodování, proti kterým selháním je nutné se bránit protiopatřeními a která naopak budou mít minoritní efekt na bezpečnostní situaci firmy. Z výsledných hodnot je pak sestavena matice. Následuje návrh opatření k zamezení nežádoucího selhání.



Obrázek 4 Postup FMEA

Zdroj 16

Analýzu prováníme především v situacích, kdy navrhujeme systém, provádíme změny v systému, jsou požadována nová opatření a když zpětná vazba od zákazníků hlásí problém.

3.1.4 Chemical Proces Quantitative Risk Analysis (CPQRA) – Analýza kvantitativních rizik procesu

Je postupem pro prognózování četnosti výsktu a následků mimořádných událostí. Tato metoda rozšiřuje kvalitativní metody hodnocení rizik o číselné vyjádření - kvantifikaci. Uplatňuje se především v oblasti bezpečnosti organizací či procesů pro chemické provozy, k čemuž byla primárně vyvinuta. Je nasazována obvykle až po jiné, méně propracované analýze a po zjištění, že tato byla nedostačující. Jedná se o jednu z nejpropracovanějších metod, reprezentující komplexní bezpečnostní studii, vyžaduje proto náročnou databázi a počítačovou podporu analýzy. Z tohoto důvodu klade značné nároky na kvalifikaci osoby zpracovatele a na čas. Pomáhá identifikovat a určit prioritu jednotlivých nebezpečí díky číselné hodnotě. Jejím prostřednictvím mohou být odhaleny kritické zdroje rizika a poté lze doporučit a navrhnout potřebná protiopatření. Pro kvantifikaci následků a dopadů je použito modelování fyzikálně-chemických procesů a jevů, jako úniky, rozptyly, požáry, výbuchy, zranitelnost příjemce rizika – modely dávek a odezvy pro koncentraci, tepelnou

radiaci, přetlak. Z těchto modelů pak vycházíme při tvorbě protiopatření, jelikož nám ukazují nebezpečné zóny při úniku chemikálie. Tyto modely tvoříme na základě hustoty osídlení v okolí, topografických charakteristik ovlivňujících rozptyl látek a efektů lokální meteorologické aktivity (například vrcholek kopce, trvale vystaven větru). Zaměřujeme se na skladovácí podmínky a přesun látek v objektu v rámci výrobní linky.

3.1.5 Human Reliability Analysis (HRA) – Analýza spolehlivosti lidského činitele

Postup pro detekci vlivu lidského činitele na výskyt mimořádných událostí. Analýza HRA pracuje s posouzením lidského faktoru (Human Factor) a lidské chyby (Human Error), tedy selhání v rozhodovacím procesu, které má za následek mimořádnou událost. Lidská chybovost je velmi specifickým parametrem, jelikož je v podstatě nepředvídatelná, existují pouze faktory jimiž můžeme přispět k jejímu snížení či zvýšení, nikdy však nemůžeme se stoprocentní spolehlivostí říci kdy selhání nastane. Úkolem HRA je tedy především identifikace zcela nežádoucích stavů a lidských selhání, která k nim mohou vést, a proto existuje přímá návazanost a souvislost s pracovními předpisy bezpečnosti práce. Pokud chceme použít metodu HRA, musíme zajistit součinnost s některou další metodou rizikové analýzy. Do výčtu a hodnocení rizik v procesu zahrnuje vliv lidského faktoru, především z pozic operátorské a rozhodovací činnosti v rámci rozsáhlých automatizovaných technologických systémů, které představují kritická místa systému kvůli rozhranní technologie - člověk. HRA má čtyři hlavní procedury. Je to vytyčení kritických míst systému, kdy určíme místa s rizikem vzniku mimořádné události a také důležité pracovní pozice. Dále kategorizujeme náročnost ovládání technologií z hlediska obtížnosti obsluhy, dělíme ji do tří stupňů. Dále vypracováváme takzvané úkolové analýzy, což jsou podrobné rozbory pracovních postupů a dílčích podúkolů nutných ke splnění určitého hlavního pracovního úkolu. Tyto analýzy jsou jednoduché, ale časově dost náročné. Posledním krokem je hodnocení faktorů ovlivňujících lidskou spolehlivost. Sem by měla patřit psychologická charakteristika pracovníka, jelikož ta je významným činitelem majícím vliv na jeho chování, což může v určitých situacích výrazně ovlivnit bezproblémový průběh rizikových situací. Tato charakteristika by měla obsahovat základní vlastnosti osobnosti, reakci na stres a úroveň pozornosti. Ačkoliv můžeme mít takto otestovaného pracovníka a ten může prospět s výbornými výsledky, nikdy si nemůžeme být jisti jeho absolutní neomylností. Některé faktory se mohou totiž vyvíjet s časem a testem

neodhalené mohou posléze vyplout na povrch, jako třeba vliv úmrtí v rodině, alkoholismus, apod. Vhodné jsou tedy průběžné kontroly, hodnocení pracovníků a pravidelné opakování analýzy.

Při HRA bychom měli taktéž provádět hodnocení pracovníků z jiného úhlu pohledu. Nikdo netvrdí, že pětkrát trestaný zloděj nemůže dosahovat v práci prvotřídních výsledků, kdy neudělá žádnou chybu. Na druhou stranu zde vyvstává riziko, zda nebude chtít uplatnit své kriminální sklony v naší firmě. Opět však musíme posuzovat případ od případu a i bývalý kriminálník může být výborným zaměstnancem, pokud mu přidělíme ideální pozici, kde není co zcizit. Ve většině případů se však tomuto riziku vyhýbáme a to i prováděním psychotestů pro určité pracovní pozice.

Do HRA lze zařadit i syndrom nespokojeného zaměstnance. Toto riziko bývá někdy opomíjeno, především ve větších firmách, kde není tolik času na řešení těchto „maličkostí“. Musíme však mít na paměti, že toto riziko je jedno z nejzávažnějších, srovnatelné s požárem či výbuchem, přestože jeho pravděpodobnost je nízká, nikoliv však nulová. Je znám případ, kdy selháním režimových opatření nebyla odebrána propuštěnému zaměstnanci papíren vstupní čipová karta a ten následně do areálu vstoupil a založil zde požár, který způsobil milionové škody. Taková sabotáž se ale dá předvídat a dalo se jí zabránit. V praxi není mnoho těchto případů, kdy nespokojenost pracovníka eskaluje k podobnému činu, přesto to neznamená, že nespokojených zaměstnanců je minimum. Naopak je jich hodně a ti pak většinou různými způsoby poškozují firmu, například rozkrádáním majetku, nedovolenou výrobou a podobně. Bohužel je to ale přirozený vývoj a pokud je zaměstnanec v práci šikanován, jsou mu neoprávněně strhávány prémie, případně je dokonce propuštěn, stane se občas, že pak za sociální tíseň, do které se dostal obviní firmu a chce se jí pomstít. Dobrý manager či ředitel podniku by proto měl velmi dobře zvážit, zda investuje do nového kamerového systému, který hlídá zaměstnance, aby nic neukradli nebo jim za ty samé prostředky dá prémie či zvýší plat, aby ke krádežím důvod neměli. Vždy je rozumnější řešit příčinu problému, než hloupě a donekonečna napravovat následky. Bohužel i dnes si stále onu příčinu mnoho lidí není schopno uvědomit.

Obrázek 5 Zaměstnanec a rozhodovací proces

Zdroj vlastní

3.1.6 CCTA Risk Analysis and Management Method (CRAMM)

Jde o metodu, která vznikla v roce 1985 v Británii jako podpora při analýze rizik informačních systémů. V současnosti je metoda implementována do nástroje (softwarového programu). Je jednou z nejznámějších metod AR pro oblast IT. Jde o software s vysokou cenou, což ho předurčuje pro odborné firmy, které se živí prováděním AR. Postup analýzy respektuje základní model z kapitoly 2.

3.2 Kvalitativní metody

Jsou jednodušší a rychlejší, slouží jako obecný přehled o rizicích, která posléze zasluhují důkladnější analýzu, uplatňuje se v ní však subjektivní vliv. Aktiva, hrozby a zranitelnosti vyjádříme v určeném rozmezí (1-10, nízké,střední,vysoké). Toto rozmezí je na nás, avšak neměli bychom jej volit zcela svévolně. Nedá se určit univerzální číslo, ale z praxe vyplývají hodnoty pro hodnotu aktiva do pěti stupňů, pravděpodobnost hrozby do čtyř, míra zranitelnosti do čtyř a úrovně rizika také do čtyř. Přičemž u rizikových úrovní musíme stanovit rozsahy pro zařazení do dané úrovně rizika. Jde o kvalifikovaný odhad, tedy konečné hodnocení určitého kritéria spočívá na schopnostech specialisty. Přesto je však

nutností, aby specialista vycházel z faktů a ověřených údajů, nikoliv aby popouštěl uzdu své fantazie. Problém nastává při zvládání rizik a finančním vyčíslení nákladů, to je ovšem cena kterou platíme za rapidně nižší spotřebu času, kterou tato metodika vyžaduje. Dle mezinárodních standardů bychom měli uvést výpočet, jakým jsme dosáhli hodnoty rizika. Výpočet je totiž možné provést více způsoby, přičemž hlavním kritériem je, aby při změně hodnot aktiva, hrozby či zranitelnosti došlo vždy ke změně hodnoty rizika. Tuto podmínku splňují dva nejčastěji používané vzorce, a to součet nebo součin jmenovaných proměnných. Tuto metodu použijeme pokud nám tento druh analýzy stačí jako podklad k rozhodnutí, anebo pokud vstupní údaje nejsou dostačující pro analýzu kvantitativní. Kvalitativní metody jsou obvykle založeny na hodnocení multioborovými respondenty, specialisty/experty, strukturovaných interview a dotazníky.
Mezi nejpoužívanější a nejznámější kvalitativní metody patří:

3.2.1 Preliminary Hazard Analysis (PHA) – Předběžná analýza ohrožení

Tuto metodu bereme jako prvotní analýzu v počátku životního cyklu zkoumaného procesu, nevylučujeme tím však možnost provedení podrobnějších analýz v dalším stádiu vývoje. Používáme ji tedy v období návrhu procesu pro ujasnění všech nebezpečí, která při něm mohou vzniknout. Díky této jedinečnosti disponuje dvěma základními výhodami, první je identifikace rizik v prvotní vývojové fázi systému a tedy jejich protiopatření stojí minimální prostředky (například změnou konfigurace systému potlačíme určité hrozby a tak ještě před sestavením a zavedením systému eliminujeme vyplývající rizika). Druhou je možnost vypracování provozních předpisů. Používají se i modifikace této metody známé pod názvy Rapid Risk Ranking a Hazard identification (HAZID).

Procedura:

Předpokladem je sestavení pracovního týmu, následuje definice a popis analyzovaného systému (jako obvykle stanovujeme hranici pro aktiva, používání a skladování energie, zvažujeme operační a přírodní podmínky, protiopatření), poté sbíráme informace z chodu podobných systémů či z databází nehod. Typickým výstupem analýzy je seznam hrozeb a jejich ohodnocení a doporučení protiopatření, seznam obsahuje i další kolonky, typické záhlaví seznamu vidíme v následující Tabulka 7.

Referenční číslo	hrozba	Riziko (co kdy kde)	Pravděpodobné příčiny	Eventuality / protiopatření	pravděpodobnost	závažnost	poznámky

Tabulka 7 Typické záhlaví výstupu PHA

Zdroj 27

V tabulce by nemělo chybět žádné riziko, jelikož podle Murphyho zákonů, které, ač jsou nepodložené vědecky, kupodivu v praxi často fungují. My bychom se měli řídit tím, který říká: „Pokud se něco může pokazit, dříve či později se tak stane“. Proto nesmíme podcenit žádné riziko i v případě, že se nám osobně zdá bezvýznamné či nedůležité. Abychom skutečně postihly všechna rizika, je vhodné použít již zpracované seznamy rizik.

3.2.2 Metoda DELPHI (delfská metoda)

Obecně

Jedna z nejpoužívanějších metod kvalitativní analýzy rizik, zároveň je i prognostickou metodou. Vznikla v 60. Letech minulého století. Definuje, co a za jakých podmínek se může stát, používá se pro tvorbu nových myšlenek. Nevýhodami jsou vysoké nároky na organizaci a časová náročnost, narozdíl od brainstormingu. Výhodami naopak menší nároky na spotřebu zdrojů a schopnost objektviního prozkoumání problematiky oprostěnou od emocí. Na rozdíl od jiných metod, pracujících se strojovým zpracováním velkého počtu dotazníků, metoda Delphi pro rizikovou analýzu používá souboru otázek, vzniklých při pohovorech. Tyto otázky musí být jednoznačné a jsou většinou tvořeny dvěmi částmi – pevnou, která je předem stanovena, a variabilní, která se mění vzhledem k průběhu pohovoru a postavení respondenta. Dotazy mají tři podoby, a to predikce budoucího stavu, zda je určitý budoucí stav žádoucí a vymezení prostředků pro předcházení nechtěného budoucího stavu. Respondenti nepřicházejí mezi sebou při práci na dotaznících do styku, proto je zaručeno určité odosobnění a vzájemné neovlivňování, zároveň však umožňuje zpětnou vazbu. Respondenty jsou experti z oborů zasažených zkoumanou problematikou, protože pro maximální úspěšnost procesu jsou nutné osoby se znalostí problematiky a letitými zkušenostmi. Základem úspěšnosti metody je proto vhodný výběr respondentů, za tímto účelem hledáme odborníky pomocí odborné literatury k danému problému, doporučení výzkumných a expertních institucí, či doporučení etablovaných pracovníků v oboru, podle úspěchů v předchozích Delphi nebo fulltextového vyhledávání. Metoda je vhodná pro nastínění budoucího vývoje, stanovení konsensu při analýze nebo k objasnení sporných témat mezi experty, dále ke stanovení společenské, ekologické, politické nebo ekonomické priority do budoucna. Data získaná z posouzení jednoho experta mají menší

vypovídací hodnotu než výstupní data získaná sloučením výsledků celé skupiny expertů. Delfská metoda je osvědčený postup slučování názorů expertů, jelikož u každé analýzy je prováděno shromáždění a hodnocení dat, na základě odpovědí expertů jsou vyhodnoceny stejné a protichůdné názory a je sestaven další dotazník. Ten by měl být sestaven takovým způsobem, aby každý expert měl možnost posoudit návrhy a názory ostatních expertů a případně pak změnit své stanovisko. Získané odpovědi jsou tedy znovu vyhodnoceny, znovu je sestaven další dotazník, který je rozeslán expertům. Cílem je co největší shoda expertů ohledně řešení daného problému. Výsledkem je poté zpracování konečné zprávy o konečném odhadu. Pokud se shody nedosáhne, otázky se mohou přeformulovat a doplnit informacemi.

Princip metody

Odhady expertů jsou upřesňovány v několika kolech, za pomoci zpětné vazby. Otázky jsou formulovány takovým způsobem, aby na ně bylo možné odpovídat kvantitativně, experti tedy musí mít k dispozici dostatečné podkladové informace pro zodpovězení. Každou odpověď by měl expert zdůvodnit. Metoda probíhá dnes formou internetové komunikace, dříve se užívala letecká pošta či fax. Tyto prostředky umožňují expertům pohodlnější práci a dovolují seskupit názory odborníků z celého světa bez nutnosti jejich osobního kontaktu, což by zároveň bylo koproduktivní a odporovalo zásadě anonymity platící pro tuto metodu. Musíme si také uvědomit, že celý proces bude trvat několik měsíců, samozřejmě to závisí na počtu kol.

Postup

Počet nezávislých expertů je od 15 do 35, jelikož očekáváme návratnost 35% až 75%. Každý expert pracuje anonymně, čímž odstraníme psychologickou bariéru, která vzniká při přímém kontaktu účastníků a potlačíme tak možnost strhnutí názorem jiného respondenta, což často pozorujeme u brainstormingu. Ustaví se řídící komise se 3 až 5 členy. Co nejpřesněji definujeme řešený problém, který následně převedeme do podoby dotazníku, kdy k jednotlivým otázkám dodáme informace pro upřesnění dotazované skutečnosti. Sestavíme seznam potenciálních expertů, získáme jejich souhlas k účasti na projektu. Organizátor zašle expertům několik dotazníků, doporučují se 2 až 3 kola, jelikož při vyšším počtu vzrůstá statistická chyba metody. Nový dotazník se zasílá vždy spolu s výsledky předešlého, statistické vyhodnocení provádí řídící komise. Na základě odpovědí

expertů jsou posouzeny shodné a odlišné názory a je vytvořen další dotazník. V každém kole může expert svůj názor na základě ostatních názorů změnit, či vysvětlit důvody k zachování starého, zároveň se vyjadřuje k odpovědím ostatních expertů. Tento postup opakujeme do doby, kdy respondenti dosáhnou určitého konsenzu, tedy shody. V praxi se většinou vždy vyskytne jisté procento expertů s určitým radikálním názorem, kteří ze skupiny vyčnívají. Konečné řešení problému prezentuje organizační tým v závěrečné zprávě.

3.2.3 Check List Analysis – Analýza pomocí kontrolního seznamu

Obrázek 6

Zdroj 34

Jedná se o nejstarší metodu pro analýzu rizik. Princip metody je založen na nalézání možné mimořádné události, která se může v systému vyskytnout. Standartně se využívá checklistu s předpřipravenými otázkami a volitelnými odpověďmi ano/ne případně ještě třetí možnost - neznámo. Příklad takového checklistu nalezneme v příloze č.1 viz str. 86. Tento typ analýzy využívá systematické kontroly splnění dopředu stanovených podmínek. Seznamy těchto podmínek, takzvané checklisty jsou tvořeny na základě charakteristických činností, které souvisejí se systémem a potenciálními dopady selhání jeho prvků a se vznikem škod. Struktura checklistu může mít formu od jednoduchého seznamu až po složitější formulář, který dovoluje zahrnout relativní důležitost parametru v rámci daného souboru. Tato procedura provádí revizi stavu systému, tedy posuzujeme shodu aktuálního stavu s požadavky norem. Metoda je vhodná k odhalení různých hrozeb, odchylek od návrhů a možných mimořádných událostí vztahujících se k vybavením a řízením procesu. Analýza

plní hodnotnou funkci při průběžné kontrole dodržování bezpečnostních nařízení, je tedy jedním z postupů, jak ověřovat určitou stránku spolehlivosti lidského faktoru ve výrobě.
Dá se říci, že jde o bezpečnostní audit, jde totiž o přezkoumání stavu bezpečnosti ve zkoumané organizaci. Je v podstatě revizí, jejímž výsledkem je konstatování zda objekt vyhověl bez výhrad (A+), vyhověl podmíněně (A), nevyhověl (B). Tímto se liší od základního modelu analýzy, jelikož závěr auditu musí být jednoznačný a vybrán z dané množiny hodnocení, aby nebyl možný rozdílný výklad. Toto hodnocení (A+,A,B) není dogmatem, ale v praxi se nejlépe osvědčilo. Audit se provádí na základě určitého vzoru:

- Auditní osnova – nejjednodušší, obsahuje nutný seznam úkolů a úkonů.
- Auditní model – je náročnější než předchozí, zavádíme model systému a hodnotíme shodu s reálným stavem. Shodu hodnotíme zpravidla podle číselné stupnice, body sčítáme a je stanoveno jaký výsledek musí být minimálně pro hodnocení A+, A a B.
- Auditní matrice – je zcela nejpřísnější metodou, kdy podobně jako u předchozího pracujeme s modelem, ten je zde však přesný, můžeme ho přirovnat k šabloně, pokud kterákoliv část šablony nesedí, výsledek je – nevyhovující. Pokud by po drobných úpravách šablona seděla, hodnotíme jako A. Pouze pokud je šablona zcela shodná s realitou, hodnotíme A+.

Při tvorbě osnovy, modelu nebo matrice musíme této činnosti věnovat maximální pozornost, jelikož výsledek radikálně ovlivní průběh a výsledek auditu samotného.

3.2.4 What If – Co se stane, když?

Obrázek 7 Generováním myšlenek více lidmi dostaneme výstup o vyšší kvalitě - princip brainstormingu

Zdroj 33

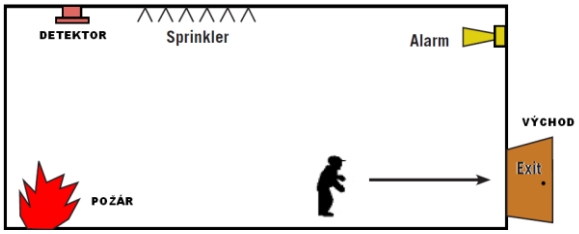
Tvůrčí metoda analýzy založená na brainstormingu. Jde o postup pro nalézání potencionálních negativních dopadů vybraných situací. V diskuzi skupina zkušených, kvalifikovaných osob, dobře obeznámených s procesem klade otázky, začínající charakteristickými slovy „Co se stane, když…..?“. V diskuzi se pak odhadují následky vzniklého stavu a samozřejmě alternativní postupy preventivních opatření s návazností na návrh konkrétního řešení snížení rizika. Předpokladem pro úspěšnost metody je odpovídající znalost procesu (provozu nebo zařízení) a aktivní účast všech diskutérů. Jde v podstatě o metodu prognostickou, pomocí níž jsme schopni analyzovat různé havarijní události či nepříjemné stavy. Metoda je časově nenáročná, avšak předpokládá profesionalitu diskutérů, přičemž je výhodou předchozí zkušenost se zaváděním této metody do praxe, pak je tato metoda vysoce účinnou při minimálním vynaloženém čase a úsilí.

3.2.5 Kombinovaná analýza typu What If s použitím Check List Analysis

Metoda je hybridem mezi dvěma již zmíněnými metodami a kombinuje jejich přednosti a potlačuje nedostatky. Slučuje se zde systematičnost kontrolního seznamu a tvořivost metody WHAT-IF. Jejím výstupem je seznam mimořádných událostí, jejich následků a protiopatření. Je často aplikována jako prvotní hodnocení a tedy předvoj podrobnější

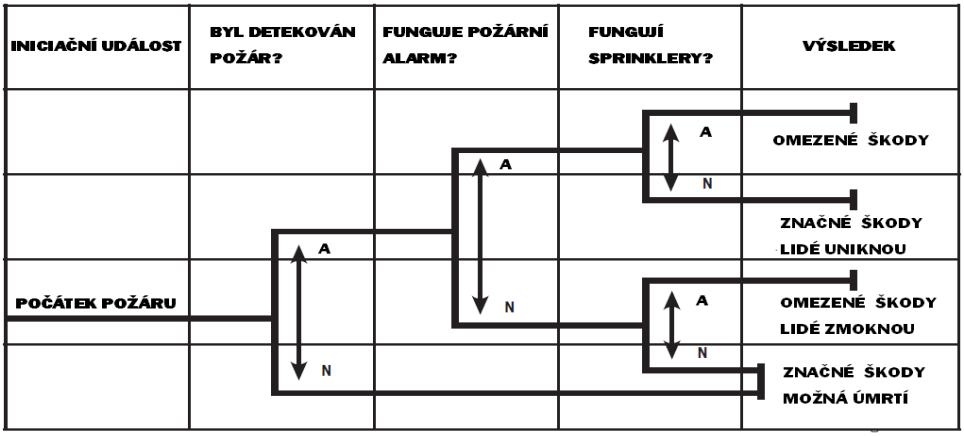
analýzy. Jako vždy je pro správnou funkčnost stěžejní, aby analytici a členové týmu měli dostatečné znalosti o zkoumaném procesu.

3.2.6 Event Tree Analysis (ETA) – Analýza stromu událostí



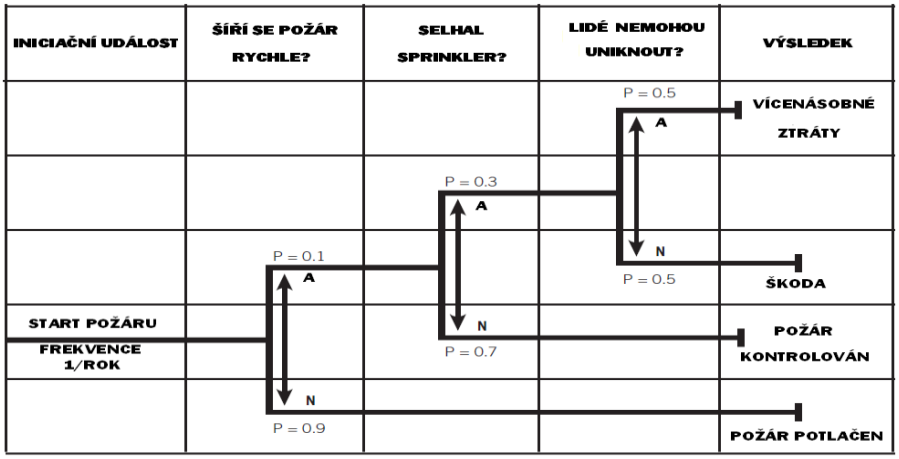
Obrázek 8 Protipožární systém

Zdroj 21



Obrázek 9 Zjednodušený strom událostí

Zdroj 21



Obrázek 10 Kvantifikace

Zdroj 21

Jde o metodu, kdy monitorujeme průběh událostí od iniciační – počáteční (selhání komponentu, nedovolený vzrůst teploty, atd.), přes následné možné cesty vývoje, pokaždé na základě dvou variant, příznivé a nepříznivé, až ke konečným následkům. Každá cesta má určenu pravděpodobnost výskytu a pravděpodobnost jednotlivých větvení lze vypočítat. Na Obrázek 8 vidíme zjednodušené schéma řešené události. Na dalším Obrázek 9 vidíme zjednodušenou rámcovou verzi analýzy. Na posledním Obrázek 10 je kvantifikovaná neboli vyčíslená varianta, kde u každého výsledku se pak zpracovává scénář s pokyny jak dále postupovat. Jde o graficko - statistickou metodu, jak vidíme v Obrázek 10, index P nám udává pravděpodobnost kladné či záporné situace. Induktivní formou rozvíjíme iniciační událost pomocí logických stavů (událost se stala – nestala nebo komponent zafungoval - selhal). Vyobrazení stromu událostí je realizováno rozvětveným grafem s dohodnutou symbolikou a popisem, za použití pravidel binární logiky stejných jako u FTA. Znázorňuje všechny události, které se v posuzovaném systému mohou vyskytnout, proto je v některé literatuře zařazena do metod kvantitativních. Postup je následovný:

1. identifikace a definice kritických iniciačních událostí
2. identifikace překážky, které mohou způsobit nahodilé události
3. tvorba stromu událostí
4. popis potenciálních výsledků iniciačních událostí
5. určení frekvence iniciační události a pravděpodobností (P) větví ve stromu událostí
6. vypočtení pravděpodobnosti pro identifikované následky
7. shrnutí a prezentace závěrů

3.2.7 Hazard and Operability Study (HAZOP) – Analýza ohrožení a provozuschopnosti

Metoda byla vyvinuta petrochemickou divizí anglické firmy Imperial Chemical Industries pro podrobnou bezpečnostní analýzu složitého technologického procesu především v oboru chemie či jemu příbuzném. Jde o metodu založenou na FMEA principu a jedná se o metodu indexovou. Zákon č. 59/2006 Sb. ukládá jako součást dokumentace v chemickém průmyslu i detailní analýzu rizika a scénáře případných nehod. Jelikož byla HAZOP vyvinuta právě pro tyto účely, je dnes na rozdíl od WHAT-IF nebo FMEA nejčastěji používanou metodou při zpracovávání dokumentace, čímž buduje pozici evropského standardu. Kvůli své propracovanosti je tato metoda časově náročná a vyžaduje pro své zpracování odborníky s odpovídajícími znalostmi, což můžeme označit za slabé stránky

metody. Její předností na rozdíl od metody WHAT-IF je systematičnost, díky které bychom neměli přehlédnout žádný významný nebezpečný stav, který může nastat. Dalšími klady metody jsou její prověřenost léty používání a tedy statut evropského standardu a také může být uplatněna ke zvýšení efektivnosti zkoumaného procesu. Metoda je založena na dvou základních předpokladech a to, že při analýze složitého procesu se často přehlédnou důležitá rizika, většinou právě kvůli složitosti, nikoliv neodbornosti analytiků. Proto je v HAZOP proces rozčleněn na podprocesy, které analyzujeme samostatně. Druhým předpokladem je fakt, že provozní hodnoty proměnných veličin, jako jsou teplota, tlak, složení, průtok, v procesu musí mít vymezen určitý rozsah, který je považován za bezpečný pro funkčnost systému, kdy odchylka od tohoto rozmezí může být nebezpečná.

Celá metoda probíhá formou brainstormingu, kdy hledáme příčiny vybočení otázkami typu „Jak se mohlo stát, že…..?“ a následky hodnotíme dotazem „Co nastane, když….?“. Dotazy však neformulujeme na základě znalostí jako u WHAT-IF, ale postupujeme systematicky podle vytvořené tabulky. Jde tedy o týmovou práci, kdy vedoucí studie diskutuje s odborným týmem, kam patří technolog, obsluha zařízení, projektant či strojní inženýr. Výsledky diskuze jsou zaznamenávány zapisovatelem do tabulky kde jsou tři základní kategorie, zdroj rizika, provozní problémy a doporučení pro prevenci.

Principem je systematická tvorba odchylek od projektovaného, funkčního stavu. Tyto odchylky se vytvářejí slovním spojením účelu zařízení s klíčovými slovy z Tabulka 8. Takto vytvoříme všechny možné odchylky, které mohou třeba jen teoreticky nastat.

Klíčové slovo	**Logický význam**	**Příklad**
NENÍ	úplná negace původní funkce	není médium v zásobníku
VĚTŠÍ	kvantitativní nárůst	větší teplota v zásobníku
MENŠÍ	kvantitativní pokles	menší teplota v zásobníku
A TAKÉ, JAKOŽ I	kvalitativní nárůst (výskyt ještě jiného případu)	průnik chladicí vody do média v reaktoru
A ROVNĚŽ	kvalitativní nárůst	zanášení topného hadu
ČÁSTEČNĚ	kvalitativní pokles	nepřítomnost některé složky
REVERZE	opačná funkce (činnost)	reverzní tok média ve výměníku

JINÝ	úplná náhrada	jiné médium v koloně
PŘEDČASNÝ	předčasná funkce (činnost)	–
ZPOŽDĚNÝ	opožděná funkce (činnost)	–

Tabulka 8 Seznam a význam klíčových slov metody HAZOP

Zdroj 32

Postup metody je tedy následovný: Rozčlenění na subsystémy, pokud možno v duchu pravidla, že jeden subsystém reprezentuje jednu funkci systému. Dále popis odchylek za použití tabulky a následná odpověď na otázku „Co mohlo způsobit, že daná odchylka nastala?“. A finálním krokem je prognóza možných následků a návrh protiopatření. identifikace nebezpečných stavů Operability study, na niž navazuje Hazard analysis, která rizika hodnotí. Výsledkem analýzy je pak nejen souhrn možných nebezpečných stavů, ale i návrh k jejich zamezení, který může být technický i organizační. Těmito opatřeními se snažíme na minimální úroveň omezit následky případného nebezpečného stavu.
Jelikož je postup metody dosti specifický, je normován v dokumentu ČSN IEC 61882 - Studie nebezpečí a provozuschopnosti (studie HAZOP) - Pokyn k použití.

3.2.8 Indexové metody

Jsou relativně nenáročné na vstupní data, umožňuji hodnotiteli „sčítat“ zdánlivě nesouvisející parametry. Výstupy těchto metod jsou takzavané indexy, které však mohou mít relativní hodnoty a je tedy nutné je pro využití nevytrhávat z kontextu. Indexové metody slouží jako podklad pro další analýzu u provozů, kde se vyskytují nebezpečné chemikálie či hořlaviny. Tyto metody pomáhají odhalovat pouze specifická rizika ke kterým jsou navrženy, nedokáží tedy analyzovat komplexně. Výstupem je odhalení míst s největším potenciálem ztráty, předpověď rozsahu poškození a ztráty přerušením provozu.

Indexovými metodami jsou:

- Dow Fire and Explosion Index (F&EI) - metoda byla vyvinuta společností Dow´s Chemical Company pro identifikaci nebezpečí požáru a výbuchu u chemických procesů. Nebezpečnost hořlavých a výbušných látek závisí na jejich fyzikálně-chemických vlastnostech a na parametrech procesu skladování či výroby.
- Mond index - je metoda zavedená společností ICI - Mond Division. Je rozšířenou verzí Dow F&EI, zahrnuje nebezpečí ohrožení toxickými látkami.

- Substance hazard index (SHI) - byl navržen Organization Resources Counselors jako nástroj pro klasifikaci nebezpečnosti látek. Index SHI je definován jako podíl rovnovážné koncentrace látky za normální teploty a prudce toxické koncentrace téže látky ve vzduchu.
- Material hazard index (MHI) - je používán ke stanovení limitního množství nebezpečné látky, které je ještě přípustné z hlediska bezpečnosti. Při překročení tohoto limitu musí být provedena bezpečnostní opatření.
- Dow Chemical Exposure Index (CEI) - je další metoda společnosti Dow Chemical Company, která ji vyvinula za účelem posouzení nebezpečí ohrožení toxickou látkou. Nebezpečnost chemických látek vyplývá především z jejich toxicity - jedovatosti. Výsledkem je stejně jako u F&EI posouzení stupně nebezpečí látky. Opět metoda přímo doporučuje hranici hodnoty indexu nebezpečnosti, při jejímž překročení mají být zdroje rizik detailněji analyzovány.
- Treshold planning quantity index (TPQ) - zavedla organizace Enviromental Protection Agency. Pro látky překračující přípustné limity množství musí být podniknuta příslušná bezpečnostní opatření.
- Rapid ranking - náleží do kategorie Relative Ranking. Umožňuje rychlou identifikaci nebezpečí požáru a ohrožení toxickou látkou.

3.2.9 SWOT analýza

Je analytickou metodou pro tvorbu strategie firmy, dokáže shrnout podstatná fakta o současném stavu do podoby, kdy na jejich základě můžeme zvolit pro nás nejvhodnější strategii. Spojuje totiž návrh bezpečnostních opatření také s faktorem financování, účelnosti, atd.

U tohoto typu analýzy identifikujeme:

- silné stránky systému (S) – všechny činnosti, které vykazují pozitivní charakter a jsou přínosné pro chod systému jako různé zdroje a dovednosti. Jedná se o spolehlivost zaměstnanců, vstupní kontrolu zamezující neoprávněnému přístupu do objektu, trvalé střežení objektu vyvedené na PCO, atd.
- slabé stránky systému (W) – znamenají nedostatky, slabiny nebo omezení, kterými systém trpí. Například nedostatečná bezpečnostní opatření, nedostatek finančních zdrojů pro jejich realizaci, atd.

- příležitosti (O) – znamenají souhrn všech potenciálních procedur, majících možnost ovlivnit příznivě náš systém. Řadíme sem rychlý dojezdový čas policie a hasičů, vhodné stavební dispozice objektu pro umístění bezpečnostních opatření, atd.
- hrozby (T) – zde tím rozumíme závažné nedostatky a možné příčiny ohrožení systému. Půjde o vysokou kriminalitu v naší lokalitě, či stavbu v záplavové lokalitě.

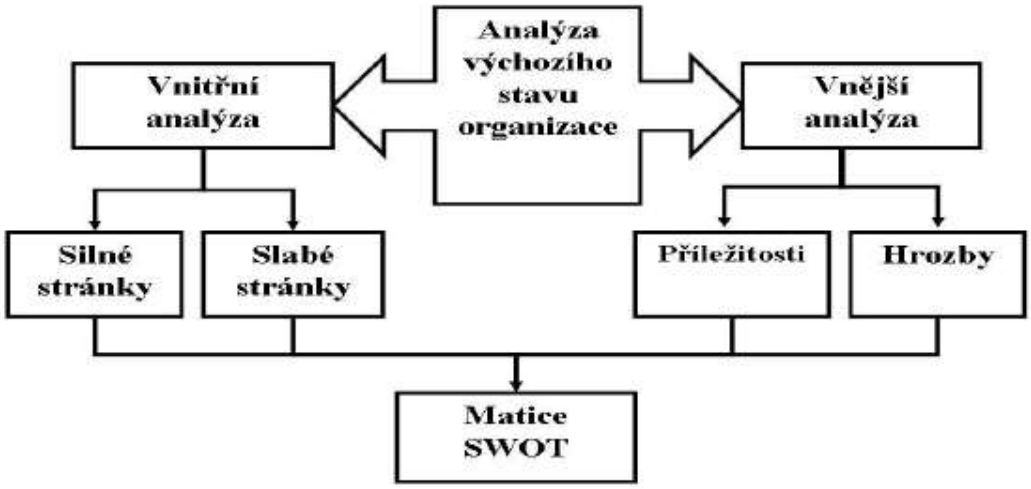
Principem metody je zařazení informací do těchto čtyř kategorií a jejich vzájemnou interakcí lze získat nové, přínosné informace. Jednotlivá pole vyplňujeme informacemi získanými brainstormingem, Delphi metodou, brainwritingem, apod. Ty jsou pak využitelné pro přeměnu slabých stránek na silné a eliminaci rizik. Na základě výstupu zvolíme pak jednu ze strategií:

- SO - využití silných stránek a příležitostí pro získání výhody (max-max)
- WO - překonání slabin využitím příležitostí (strategie min-max)
- ST - využití silných stránek na obranu proti hrozbám (strategie max-min)
- WT - minimalizování nákladů a čelení hrozbám (strategie min-min)

Účelem SWOT tedy není identifikace maximálního počtu silných a slabých stránek či příležitostí a hrozeb. Účelem je identifikovat problémové oblasti a definovat směr, kterým se v těchto oblastech chceme ubírat. Po provedení SWOT analýzy a zvolení jedné ze čtyř strategií musíme následně stanovit konkrétní postupy, jakými chceme požadovaného cíle dosáhnout.

V podstatě je SWOT analýza složena ze dvou separovaných analýz, a to interní analýzy, kde hodnotíme slabiny a silné stránky a externí analýzy kde provádíme hodnocení hrozeb a příležitostí.

Postup:

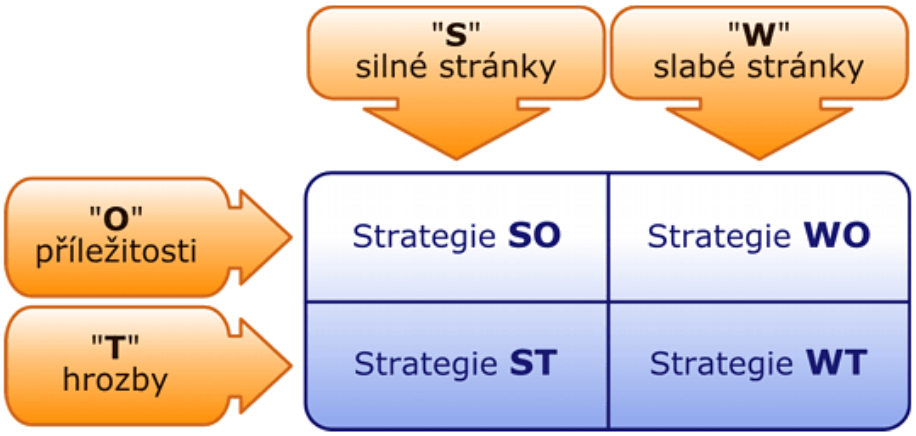


Obrázek 11 Postup SWOT

Zdroj 12

Nejprve tedy provedeme interní analýzu, vymezíme oblasti, ve kterých budeme slabé i silné stránky hledat a určíme pracovní skupinu odborníků, kteří například brainstormingem vygenerují seznam silných a slabých stránek z vymezených oblastí. Z těchto stránek pak dále redukujeme jejich počet pouze na ty významné a stěžejní a jim přiřazujeme důležitost (velmi slabé až velmi silné). Dále v každé oblasti seřadíme stránky dle priority – významnosti pro tuto oblast (přičemž priorita 1 značí nejvyšší hodnotu).

Ve druhé fázi provádíme externí analýzu, postupujeme obdobně jako u analýzy interní. Opět sestavíme tým odborníků, kteří identifikují příležitosti a hrozby v daných oblastech, dále určují jejich možný dopad a pravděpodobnost s jakou mohou nastat. Poté vpisujeme získaná data do matice hrozeb a do matice příležitostí, následně seskupujeme všechna zjištěná fakta do matice z Obrázek 12, přičemž dodržujeme pořadí priorit. Následně volíme jednu ze zmíněných strategií pro řešení problémů a přistupujeme k zavádění opatření do praxe.



Obrázek 12 SWOT analýza

Zdroj 31

3.3 Vlastní metody

Pro analýzu rizik si můžeme dokonce vytvořit metodu vlastní. Musíme se pouze držet pravidla, že při změně hodnoty aktiva, hrozby či zranitelnosti se musí změnit hodnota rizika. Zároveň bychom měli zajistit možnost opakovatelnosti měření. Zásadní výhodou při zvolení vlastního postupu je možnost zkonstruovat analýzu na míru našemu prostředí, nevýhodou je pak opakovatelnost v odlišných podmínkách (jiném provozu). Nedoporučuje se tvořit vlastní metodu bez předchozích zkušeností.

4 BEZPEČNOSTNÍ ANALÝZA PŘED ZAPOČETÍM STŘEŽENÍ OBJEKTU BEZPEČNOSTNÍ AGENTUROU

Jak bylo řečeno na začátku práce, tato analýza v podstatě spadá pod komplexní BA podniku. S tím rozdílem, že ji provádí jiný subjekt – bezpečnostní agentura najatá firmou. Pokud z bezpečnostní politiky podniku či BA vyplyne, že je třeba objekt firmy střežit pomocí fyzických či technických prostředků, zadá firma tuto práci právě bezpečnostní agentuře. Výstupem takovéto práce je souhrn bezpečnostních poznatků majících značný vliv na způsob ochrany objektu, například: továrna na okraji vesnice, zaměstnávající bývalé trestance, bez jakékoliv technické či fyzické ostrahy, absence požární ochrany a MZS, již čtyřikrát vykradena. Tento souhrn je podkladem a vodítkem pro bezpečnostní agenturu, aby mohla nasadit účinná technická opatření a fyzické síly pro ochranu objektu. Před nasazení fyzické ostrahy či podnikových detektivů využívají agentury vhodné metodiky analýzy, popsané v kapitole 3. Přičemž osnova takové analýzy a okruhy, na které je nutné se při zkoumání objektu z bezpečnostního hlediska zaměřit, mohou vypadat dle praktických zkušeností JuDr. Z. Materny takto:

Obecné informace - Název firmy a sídlo, IČ, DIČ, kontaktní osoby.

Bezpečnostní politika – průhlednost hospodaření, externisté

Legislativa týkající se podniku

Provozně-organizační charakteristika – druh činnosti subjektu (peněžnictví, průmysl, chemie, služby), topografické aspekty (na kraji/ve středu obce, samota, údolí, vrcholek, rovina, hustota zástavby, dopravní dostupnost, přístupy), časové aspekty (ruch a provoz v okolí objektu a přímo v objektu – otevírací doba, přístup veřejnosti), demografické aspekty vně objektu (trestaní, sociálně nepřizpůsobiví, excesy, tuzemci, cizinci, věk osob), demografické aspekty uvnitř objektu (vzdělanostní úroveň, trestaní, sociálně nepřizpůsobiví, excesy, pracovní kolektiv – věk, tuzemci/cizinci), předcházení protiprávní činnosti (ano/ne), globální rizika (lidská činnost, přírodní jevy, havárie, pojištění proti těmto jevům), vstup a kontrola pohybu osob, materiálu a informací (celkový počet zaměstnanců, externistů, vozidel, počet vstupů, výstupů, vjezdů, výjezdů, kontrolní body pohybu, propustkové body, kontrola zavazadel kde a komu a zda je vůbec prováděna, osobní kontrola, průkazy zaměstnanců, dodavatelů, návštěv, evidence průchodů a průjezdů, kontrola vozidel, osádek), hlídací služba (statická, pohyblivá, psovod, pes, klíčová služba,

přeprava cenností, počty osob na směnách, fluktuace, výstroj, výzbroj, spojovací technika), úklid (fluktuace, počty, čas úklidu, dokumentace, doprovod + kontrola), klíčový a uzavírací režim (centrální uložení náhradních klíčů, způsob uložení klíčů, vydávání klíčů a dokumentace), ochrana informací (interní normy, obsah a forma dokumentů, seznam osob určených pro nakládání s těmito informacemi, prověrky, školení, kontrola, sankce, evidence, zneužití, zkopírování, spolupráce s PČR), Data na PC (individuální, síťová ochrana, přístupová práva, vyjímatelné HD, hesla, antivir), speciální režimová pracoviště (místnost porad – odposlechy, archiv, spisy), řadová režimová pracoviště (pokladny, účtárny, dispečink), požární ochrana, BOZP, organizace a řízení režimu v nestandartních situacích (kompetence, dokumentace, krizový štáb, evakuace, nácvik),

opatření v oblasti lidských zdrojů – připravenost na zvládání krizových situací (sabotáže, teror, občanská válka, politické nepokoje, obecné ohrožení, krádež vloupáním, výtržnosti, graffiti, vandalismus, pohružka bombou, vniknutí do objektu násilím/lstí, únik informací, úplatkářství, drogy, alkohol), loajalita stálých i externích pracovníků (ztotožnění s cíli organizace, sociologické a psychologické průzkumy, personální pohovory, pravidelná hodnocení, kontroly pracovišť a dodržování režimových opatření, vyhodnocování telefonních hovorů, emailové komunikace)

stavebně technická opatření – stavba a stavební prvky (obvodové a nosné konstrukce, oplocení, luxfery, okna, výlohy, okenice, bezpečnostní žaluzie, rolety, fólie, skla, světlíky, větrací otvory, dveře vrata, mříže, kování, balkóny, venkovní schodiště, požární žebříky, střecha a vstupy skrz ni, sklepy a jejich zajištění), externí stavby jako přístřešky na kola, garáže, apod. , technologická zařízení a záložní zdroje (kotelna, trafostanice, výměníková stanice, sklad plynových lahví, úpravna vody, strojovna klimatizace, strojovny výtahů, záložní zdroje elektřiny, telefonní ústředna), inženýrské prvky a rozvody (výtahy, interkom, počítačová síť, hlavní telefonní kabel, přívod tepla, teplé a studené vody, plynu, elektřiny a jejich rozvody, hasící přístroje a agregáty, svody kanalizace a odpadové šachty), klasifikace místností a prostor (chodby, koridory, haly, turnikety, schodiště, zazděné místnosti, prostory za obložením stěn, kanály pro inženýrské sítě, místnosti zajištěné proti odposlechu) ostatní režimová pracoviště (sekretariáty, spisovny, dílny, sklady, prodejny, výdejny, laboratoře, rozložení bytu), vybavení interiérů (plakáty, nábytek, záclony, závěsy, žaluzie, elektrické vybavení), integrální součásti interiérů (ústřední topení, klimatizační

tělesa, osvětlovací tělesa, zásuvky, reproduktory interkomu), součásti exteriérů (odpadkové koše, bufetové stánky, altány, vstupy do kanálů).

materiálně technická opatření – soubor materiálně technických opatření (základní údaje, účel a filozofie systému, projektová dokumentace, použité normy, integrace systému), materiálně technické vybavené relevantní pro bezpečnost (komorové a mobilní trezory, bezpečnostní skříně a speciální schránky, zařízení k vyhledávání nelineárních přechodů, rušičky, PZTS, EPS, kamerové systémy, vstupní systémy, turnikety, karty, čipy, klíčové systémy, perimetrické systémy, chemické a fotochemické nástrahy, mechanické nástrahy, nouzové osvětlení, MZS, záložní zdroje, záznamová média, listiny a dokumenty), Závěry a doporučení (filozofie systému, kompatibilita prvků, odolnost systému vůči destrukci, integrita systému, certifikace, operativní a strategická doporučení).

Tento výčet není kompletní a obsahuje pouze heslovitá klíčová slova, předpokládá se, že odpovědná osoba dokáže text náležitě analyzovat a vyvodit z něj všechny otázky, které se budou týkat bezpečnosti objektu. Jako vždy není seznam zcela kompletní a je vždy nutné analyzovat situaci na místě pro maximální přesnost analýzy. V praxi se vyplatilo identifikovat zdroje rizika pomocí statistické analýzy mimořádných událostí jako vloupání, krádeže, požáry, žhářství, za období posledních 3 až 5 let.

Pro předběžnou analýzu před nasazením PZTS lze použít postup dle normy ČSN CLC/TS 50131-7:

4.1 Bezpečnostní posouzení objektu

Jde o činnost v rámci návrhu PZTS. Před vlastním návrhem se musíme seznámit s objektem, a všemi působícími vlivy. Zvláště důležité bude jednoznačné vymezení způsobu užívání objektu a případně požadavky na členění přístupu do jeho jednotlivých částí. Je velmi přínosné získat kopii výkresové stavební dokumentace objektu. Při posuzování objektu stupně 1 a 2 se doporučuje vyplnit formulář „Protokol bezpečnostního posouzení objektu“ viz příloha 2. Údaje z tohoto formuláře pak poslouží při návrhu systému. Bezpečnostní posouzení objektu je analýzou, kterou provádíme za účelem zjištění:

- rozsahu systému (počet komponentů)
- východiska pro volbu komponentů - identifikovat faktory ovlivňující volbu a umístění bezpečnosních komponentů (detektorů, ústředny, kabeláže).

- stupně zabezpečení –Pro instalaci je pak možné použít i prvky s vyšším stupněm zabezpečení, nikdy však s nižším, jelikož platí pravidlo nejslabšího článku řetězu. Dle normy ČSN CLC/TS 50131-1 určujeme předpokládaný stupeň rizika objektu takto:

  - Stupeň 1: Nízké riziko. Předpokládá se, že vetřelec nebo lupič mají malou znalost PZTS a mají k dispozici omezený sortiment snadno dostupných nástrojů.
  - Stupeň 2: Nízké až střední riziko. Předpokládá se, že vetřelec nebo lupič mají omezené znalosti PZTS a používání běžného nářadí a přenosných přístrojů (např. multimetr).
  - Stupeň 3: Střední až vysoké riziko. Předpokládá se, že vetřelec nebo lupič je obeznámen s PZTS a mají rozsáhlý sortiment nástrojů a přenosných elektronických zařízení.
  - Stupeň 4: Vysoké riziko. Používá se, má- li zabezpečení prioritu před všemi ostatními hledisky. Předpokládá se, že vetřelec nebo lupič jsou schopni nebo mají možnost zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponentů PZTS.

Střeží se	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Obvodové dveře	O	O	OP	OP
Okna		O	OP	OP
Ostatní otvory		O	OP	OP
Stěny			P	P
Stropy nebo střechy			P	P
Podlahy				P
Místnosti	T	T	T	T
Objekt (vysoké riziko)			*S*	*S*

O-otevření P-průnik T-past (nástraha) *S* - objekty vyžadující speciální pozornost

Tabulka 9 Stupně zabezpečení

Zdroj 12

Stupeň zabezpečení pro který je zařízení určeno, je stanoven výrobcem v technických údajích o zařízení, přičemž norma ČSN CLC/TS 50131 stanovuje kritéria pro zařazení do jednotlivých stupňů . Narozdíl od této klasifikace zařízení do stupňů zabezpečení normou,

neexistuje jednoznačný předpis, jenž by zařazoval jednotlivé objekty do míry rizika. Při návrhu vhodného stupně PZTS je proto nutné zvážit více aspektů (hodnotu majetku, jeho důležitost, lokalitu apod.). Obecně lze říci, že obytné objekty jako byty a rodinné domy obvykle spadají do stupně 1 až 2. Obchody, restaurace, sklady, kanceláře, dílny, a další prostory, ve kterých není uložen drahý majetek jsou většinou zařazovány do stupně 2. Místa, kde se nachází velké objemy peněz v hotovosti, drahé šperky, omamné látky a podobně se řadí nejčastěji do stupně 3. Do stupně 4 se pak řadí strategicky důležitá místa (tiskárny cenin, zpracování diamantů, zlata apod.). Nejčastěji se tedy v praxi setkáme se stupněm 2. Zařazení objektu do daného stupně provádí dodavatel na základě požadavků a upřesnění objednatele a dalších kompetentních účastníků.

- třídy prostředí

Je také nutné určit charakteristiku prostoru, do kterého budou zařízení montována. Z tabulky je zřejmé, že objekt firmy může být rozčleněn na jednotlivé úseky, v nichž bude stanovena jiná třída prostředí. Třídu je nutno určit pro správný výběr komponentů, aby byly schopny provozu v daných podmínkách. Třídu uvádí výrobce komponentu v dokumentaci k výrobku.

Třída	Název prostředí	Popis prostředí, příklady	Rozsah teplot
I	**vnitřní**	Vytápěná obytná nebo obchodní místa	+5 °C až +40 °C
II	**vnitřní všeobecné**	Přerušovaně vytápěná nebo nevytápěná místa (chodby,schodiště, skladové prostory)	-10 °C až +40 °C
III	**venkovní chráněné**	Prostředí vně budov, kde komponenty nejsou trvale vystaveny vlivům počasí (přístřešky)	-25 °C až +50 °C
IV	**venkovní všeobecné**	Prostředí vně budov, kde komponenty jsou trvale vystaveny vlivům počasí	-25 °C až +60 °C

Tabulka 10 Třídy prostředí

Zdroj: 24

- návrhu řešení systému (počty, typy detektorů, apod.)

Vycházíme z norem řady 50131. Je však velmi důležité si uvědomit, že následující postup analýzy je pouze doporučením a zároveň neposkytuje návod k činnostem v rámci návrhu systému. Jelikož uvedené výčty nejsou a nebudou nikdy kompletní (především díky rozmanitosti různých objektů a tím i faktorů, které v nich působí), jsou při této práci neocenitelné zkušenosti z praxe jakožto i bezpečnostní čich zpracovatele. Norma tedy

slouží jako podklad pro zpracování analýzy objektu, avšak záleží na zpracovateli, jaká nebezpečí a slabá místa odhalí nad rámec faktorů uvedených v normě.

Analýza má tyto hlavní části:

4.1.1 Posouzení aktiv

V první fázi identifikujeme a oceňujeme zabezpečované hodnoty. Jelikož míra pravděpodobnosti napadení objektu závisí na charakteru aktiv. Dle ČSN CLC/TS 50131-7 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy, část. 7: Pokyny pro aplikace. Příloha B, posuzujeme především:

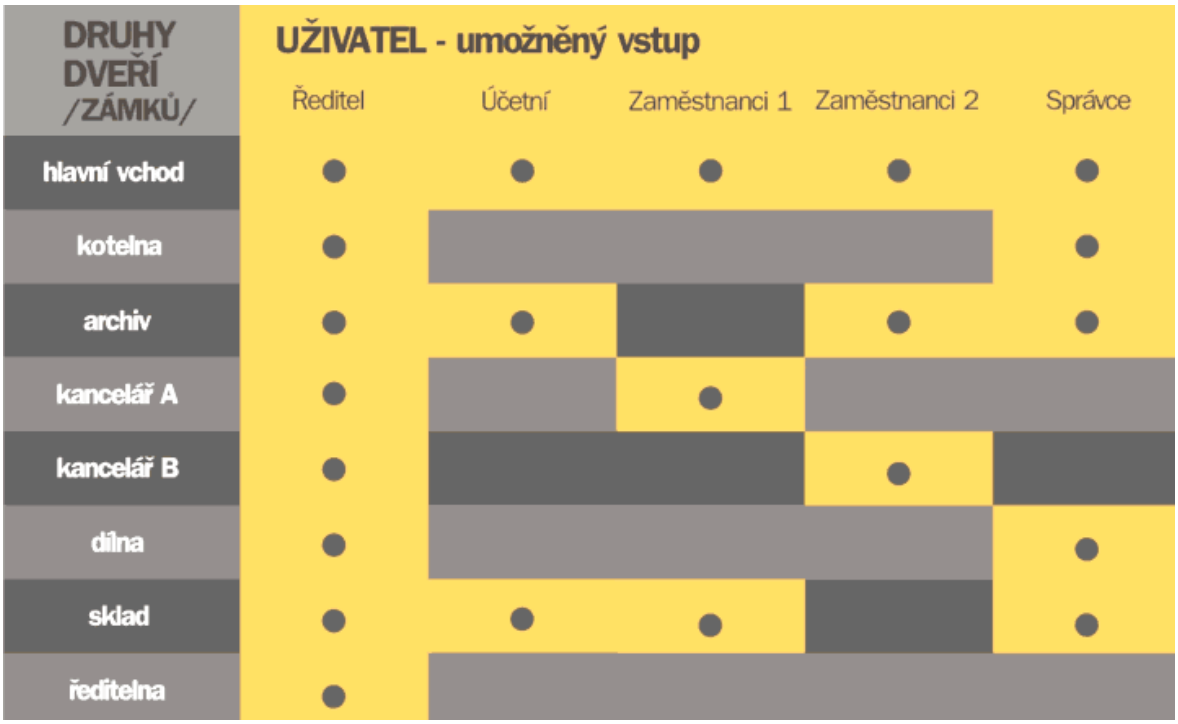
- Druh majetku – zde se soustředíme na atraktivitu, snadnost zpeněžení aktiv.
- Hodnota majetku – znamená maximální hodnotu přímé ztráty, osobní vztah k majetku, náklady vztahující se ke ztrátě či poškození.
- Objem majetku – sem patří náročnost odcizení a přepravy (rozdíl, zda jde o disk s daty či bagr), tržní aktraktivita.
- Historie napadení – zde analyzujeme četnost a způsob napadení.
- Nebezpečí – Jde o nebezpečí zneužití aktiva (radioaktivní materiál pro výrobu špinavé bomby), dále nebezpečnost pro osoby (vzácný jedovatý had), nebezpečnost pro okolí (toxický materiál).
- Poškození aktiv – žhářství, vandalismus, činnost nespokojených zaměstnanců.

4.1.2 Posouzení budovy

Podstatné rozdíly ve skladbě systému a způsobu střežení pramení z rozdílného charakteru fyzické struktury budovy (jinak budeme zabezpečovat rodinný dům narozdíl od letiště). Cílem je zde identifikovat slabá místa v rámci stavebních dispozic objektu, která mohou být zneužitelná pro napadení. Dle ČSN CLC/TS 50131-7 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy, část. 7: Pokyny pro aplikace. Příloha C hodnotíme zejména:

- Konstrukci – obecně plášť střeženého prostoru (stěny, střechy, podlahy, stropy)
- Otvory – okna, dveře, střešní světlíky, ventilační šachty, servisní vstupy jako kanalizace, výtahové šachty apod.

- Provozní režim objektu - doba osídlenosti objektu, jako přítomnost ostrahy, přístupové možnosti veřejnosti, návštěv, exkurzí, apod.
- Majitelé klíčů – zejména u středních a větších firem by měl fungovat určitý řád, určující kdo bude mít kam přístup. Možné rozdělení vidíme na Obrázek 13.



Obrázek 13 Držitelé klíčů – příklad

Zdroj 12

- Lokalita – kriminalita v dané oblasti, vzdálenost od dalších objektů (chata na samotě u lesa, výrobní hala uprostřed aglomerace), dojezdový čas zasahujících složek po vyhlášení poplachu, vliv sousedních budov na možnost napadení.
- Stávající zabezpečení - kvalita a rozsah MZS a PZTS.
- Historie krádeží, loupeží, výhružek - počet předcházejících incidentů, způsob jejich realizace.
- Místní legislativa a předpisy - bezpečnostní požadavky, požární předpisy, požadavky vzhledem ke konstrukci objektu. Například pro objekty, kde jsou zpracovávány či uchovávány UI je vyžadován minimální stupeň zabezpečení závislý na stupni utajení.

- Prostředí střeženého objektu - městská zástavba, venkov, typ osídlení, přírodní překážky, nadmořská výška, reliéf krajiny, apod.

4.1.3 Vlivy působící uvnitř objektu

Jedná se o faktory ovlivnitelné majitelem objektu, které mají stěžejní význam pro umístění komponentů bezpečnostního systému. Dle ČSN CLC/TS 50131-7 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy, část. 7: Pokyny pro aplikace. Příloha D.

- Vodovodní potrubí - vliv pohybu vody v plastových potrubích ovlivňuje nasazení mikrovlnných detektorů.
- Vytápění, vzduchotechnika, klimatizace - vliv turbulence vzduchu např. na nasazení ultrazvukových detektorů.
- Vývěsní štíty, zavěšené předměty - vliv zavěšených předmětů s možností pohybu v zorném poli detektorů (záclony, rostliny, lampy, reklama), ovlivňuje nasazení PIR detektorů.
- Výtahy, vliv vibrací strojních zařízení (např. otřesová čidla)
- Zdroje světla - Kompaktní výbojky, zářivky mají vliv na rušení mikrovlnných detektorů, bodové reflektory, nasměrované na čočky (zrcadla) PIR detektorů, vliv světlometů vozidel, slunce.
- Elektromagnetické rušení – všechna elektronická zařízení mohou být zdrojem rušivých signálů, odhalujeme zde potencionální zdroje záměrného i neúmyslného EM rušení. EM rušení znamená vyzařované, po vedení, ale i elektrostatické výboje. Příkladem jsou svářecí zařízení, zařízení obsahující elektromotor, výbojky.
- Vnější zvuky - v případě nasazení ultrazvukových detektorů (telefonní zvonky, netěsnosti vzduchových potrubí, kompresory)
- Domácí zvířata - vliv na detektory pohybu, jejich nasměrování, případně volbu čočky u PIR.
- Průvan - citlivost detektorů na proudění vzduchu, u ultrazvukových detektorů je zvuk mediem pro přenos energie, u PIR při rychlé změně teploty nastává tepelný šok a aktivace poplachu. Důležité jsou i těsnění stavebních otvorů, závěsné,

pohybující se předměty jako plakáty, rostliny, závěsy, které vlivem průvanu vyvolávají pohyb.

- Uspořádání skladovaných předmětů - z hlediska zastínění zorného pole detektoru (například víme že dosud prázdný prostor bude sloužit jako skladiště a bude tedy značně zaplněn), možnost uvolnění předmětů a jejich následný pohyb.
- Stavební konstrukce střežených objektů - střechy, stěny, podlahy, sklepy, lehké stavební materiály mohou vibrovat, stav a usazení dveří, oken.
- Umístění detektorů na zasklení - složení skla (dvojsklo, vrstvené, kalené), možnost vyjmutí skla z rámu (riziko u starších zasklení, kdy sklo v rámu drží pouze gumová lišta, kterou lze bez potíží vyjmout a následně vytáhnout celou tabuli bez poškození a hluku), teplotní rozdíly na povrchu skla, kondenzace vody.
- Riziko planých poplachů u tísňových zařízení - volba umístění detektorů z hlediska pohybu osob, možná aktivace dětmi.

4.1.4 Vlivy působící vně objektu

Jde o faktory, které obvykle majitel objektu nemůže změnit či potlačit. Dle ČSN CLC/TS 50131-7 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy, část. 7: Pokyny pro aplikace. Příloha E.

- Dlouhodobě působící faktory – jsou takové, u kterých nepředpokládáme změnu řádově v rocích, jde o silnice, železnice, metro, parkoviště, letecký koridor, seizmická rizika- podloží, apod.
- Krátkodobě působící faktory - výstavba
- Vlivy počasí - převažující a potencionální vlivy počasí, exponovaná místa větru, dešti, pobřeží, kopce, blesky.
- Vysokofrekvenční rušení - vysílače TV, rozhlasové, základnové stanice GSM, radary, vliv na bezdrátové komponenty EZS
- Sousední objekty - vibrace, EM rušení, průmyslové objekty.
- Vlivy klimatických podmínek - výběr zařízení odpovídající místním klimatickým podmínkám (tedy teplota, vlhkost)

- Ostatní vnější vlivy - aktivity v přístupných vnějších částech objektu, aktivity v přilehlých částech rozsáhlejších komplexů budov, jako hrající si děti, kulturní, sportovní akce.

Po bezpečnostním posouzení objektu následuje fáze přípravy realizace a následně samotná montáž PZTS.

II. PRAKTICKÁ ČÁST

5 BEZPEČNOSTNÍ ANALÝZA FIRMY XY

V praktické části této práce uvedu bezpečnostní analýzu konkrétní instituce. Bude se jednat o provozovnu čajovny, tato není dosud zkolaudována. Z důvodu, že tato práce bude veřejně přístupnou a tedy informace v ní obsažene by mohly být zneužity při konkurenčním boji či podvratnými živly, nebude zde uvedena žádná informace, která by mohla vést k identifikaci objektu zde popisovaného.

Do prostoru provozovny se vstupuje dveřmi do chodby 01, dalším standartním vchodem jsou dveře na schodiště v chodbě 17, tyto budou však využívány výhradně provozovateli a budou neustále uzamčeny. V místech 02, 04, 03 a 18 jsou prostory pro hosty. Prostor 16 bude sloužit jako šatna a bude uzamykán. Prostor 19 bude přípravnou dýmek a zároveň menším skladem, taktéž bude uzamykán.

Nejprve v rámci studie definujeme problém, bude se jednat o ochranu bezpečnostních zájmů pro společenský podnik – čajovnu. Čajovna se nachází v suterénu obytného domu, půdorys je obsažen v 88, svou velikostí pojme zhruba 30 hostů plus personál. Jelikož se nejedná o příliš rizikový provoz, obsahové nároky tomu budou odpovídat. Časové nároky na zpracování jsou jasně dány termínem odevzdání této DP, tedy 27.5.2011. Finanční nároky na zpracování analýzy jsou samozřejmě z mé strany nulové, ocenil jsem však čas strávený analytickou činností, aby měl čtenář představu na kolik by podobná analýza vyšla. Cena práce za hodinu se zde pohybuje od 500 do 3000 korun, suma je závislá na složitosti analýzy. V závěru analýzy jsou shrnuta doporučení protiopatření včetně jejich ekonomické rozvahy.

Následně jsem provedl dle požadavků majitele kvalitativní analýzu:

5.1 Analýza aktiv

Finanční hranici pro zahrnutí aktiv do analýzy určil majitel na 1500,- Kč. Volíme 4 stupně ocenění hodnoty aktiva (malá, střední, velká, neocenitelná). Dostáváme tato aktiva:

- Zboží – využijeme možnost seskupovat aktiva (zejména díky společným skladovacím prostorům) a zařadíme pod tuto položku tabáky, čaje, kávy a nápoje. Hodnota – malá - 1.

- Vybavení – opět sekupujeme pro zjednodušení a řadíme sem sklo, keramiku, dekorace, nábytek, elektroniku. Hodnota – střední - 2.
- Vodní dýmky – zase seskupujeme, jedná se o jednu z nejcennějších složek vybavení, proto ji od ostatního vybavení separujeme. Hodnota - střední - 2.
- Dobrá pověst podniku – aktivum nevyčíslitelné hodnoty, pokud podnik bude mít špatnou pověst a nebude navštěvován zákazníky, postupně upadne a zkrachuje. Hodnota – neocenitelná - 4.
- Zdraví a bezpečnost osob – týká se osob pohybujících se v prostorách čajovny, tedy návštěvníků i personálu. Hodnotím stupněm hodnoty – velká - 3.

5.2 Analýza hrozeb

Hodnotíme úroveň hrozby ve 4 stupních (malá, střední, vysoká, kritická). Mezi nejzávažnější identifikované hrozby v objektu patří:

Požár – jelikož se jedná o prostory, kde se bude každodenně manipulovat s vodními dýmkami, prostor též vytápí dvoje kamna na tuhá paliva, která mohou být též zdrojem požáru. Úroveň – střední - 2.

Žhářství – úmyslně založený požár lze předpokládat kvůli blízkosti dalších čajoven a konkurenčnímu boji. Působí stejný dopad jako běžný požár, ale má odlišného iniciátora, proto je nutné je od sebe odlišit. Úroveň – kritická - 4.

Krádež vloupáním – Přestože v objektu nejsou uložena aktiva nějaké obrovské hodnoty, může dojít k jeho napadení. Úroveň – střední - 2.

Krádež aktiva a vynesení z provozovny - Úroveň – vysoká - 3.

Útěk zákazníka bez placení – bohužel v dnešní době nijak zvláštní jev, jelikož jeho iniciátorem je člověk, jeho výskyt je těžké určit. Úroveň – malá - 1.

Nehoda – bude se jednat zejména o popáleniny při manipulaci s dýmkami či kamny, jiné nehody se nepředpokládají. Úroveň – malá - 1.

V podniku se nebude podávat alkohol, takže odpadají starosti s opilými hosty, kteří tak netvoří hrozbu, že by mohli zranit sebe či ostatní nebo poškodit vybavení provozovny.

5.3 Analýza zranitelností

Použijeme 4 stupně hodnocení (nízká - 1, střední - 2, vysoká - 3, kritická - 4). Tvoříme dvojice aktivum – hrozba a oceňujeme zranitelnost každé této kombinace, hodnotíme dle citlivosti a kritičnosti.

číslo	aktivum	hrozba	zranitelnost
1	zboží	Krádež vloupáním	3
2	vybavení	Krádež vloupáním	3
3	dýmky	Krádež vloupáním	3
4	dýmky	Krádež vynesením z provozovny	3
5	Dobrá pověst podniku	Nehoda	2
6	Zdraví a bezpečnost osob	Nehoda	2
7	Zdraví a bezpečnost osob	požár	2
8	zboží	požár	4
9	vybavení	požár	4
10	dýmky	požár	4
11	zboží	Žhářství	4
12	vybavení	Žhářství	4
13	dýmky	Žhářství	4
14	zboží	Útěk zákazníka bez placení	2

Tabulka 11 Hodnocení zranitelností

Zdroj vlastní

5.4 Stanovení výše rizika

Pro výpočet rizika jsem zvolil součin hodnoty aktiva, hrozby a zranitelnosti, jak je vyjádřeno v tabulce . Rizika jsem pak zařadil do jedné z kategorií – banální (0-10), střední (11-20), vysoké (21-30), fatální (31-40). Vzorec pro výpočet je R=A*H*Z.

číslo	aktivum	hrozba	zranitelnost	riziko
1	1	2	3	6
2	2	2	3	12
3	2	2	3	12
4	2	3	3	18
5	4	1	2	8
6	3	1	2	6
7	3	2	2	12
8	1	2	4	8
9	2	2	4	16
10	2	2	4	16
11	1	4	4	16

12	2	4	4	32
13	2	4	4	32
14	1	1	2	2

Tabulka 12 Hodnocení rizik

Zdroj vlastní

5.5 Vyhodnocení rizik

Největším rizikem je tedy škoda způsobená požárem, a to jak běžným, tak žhářstvím. Tato událost by nejen zničila kompletně interiér provozovny, ale zároveň by zneschopnila provoz podniku, což by znamenalo sekundární ztráty. Budeme však řešit všechna rizika z tabulky, abychom ukázali možnost komplexního řešení zabezpečení, zároveň je to přání majitele.

5.6 Návrh optimalizace

Jelikož stávající protiopatření vůči rizikům jsou slabší, doporučuji:

- Použití EPS pro prevenci požáru v objektu. Pro ušetření nákladů na samostatnou EPS doporučuji kombinovaný bezdrátový systém spolu s PZTS. Tato kombinace má také obecné výhody bezdrátového systému, tedy nemusíme řešit problematiku kabeláže a tak ušetříme za montážní práce (vzhledem k tomu, že objekt je již téměř zcela vybaven, stěny natřeny, jde o velkou výhodu, protože nemusíme opět vysekávat drážky), dále může být systém lehce rekonfigurován a rozšiřován (toto lze předpokládat, jelikož v budoucnu je možné na systém navázat při zabezpečování bytu majitele, který se nachází nad čajovnou). Hlásiče budou duální, jelikož v objektu se bude kouřit a budou nastaveny pouze na teplotní čidlo (kouřové bude vypnuto), toto opatření je z důvodu omezeného výběru hlásičů pro daný systém. S reakcí teplotního čidla nebudou žádné potíže, jelikož celý prostor je vybaven spoustou hořlavých dekorací a nábytku a tím při zapálení dochází k rapidnímu nárůstu teploty, na což čidlo reaguje. Doporučuji použití bezdrátového řešení pomocí systému JA-6x od společnosti Jablotron. Teplotní hlásiče jsou v půdorysu zelenou barvou.
- Pro ochranu zdraví osob doporučuji vybavit prostory lékárničkou, zejména s prostředky na popáleniny a tišení bolesti.

- Použití MZS pro zvýšení ochrany vůči nedovolenému přístupu do prostoru čajovny. Na vybraná okna a dveře doporučuji instalaci mříží z vnitřní strany (v půdorysu zaznačena modře), což podstatně ztíží průnik pachatele do objektu, na rozdíl od instalace mříží z venkovní strany (pachatel musí nejprve překonat okno či dveře, teprve poté má přístup k mříži, u oken již při jejich rozbití zareaguje glass break detektor či PIR, plní tedy v podstatě funkci předpoplachu). Jelikož v objektu budou časem vyměněna okna, je zbytečné investovat do bezpečnostních skel a volíme raději, bohužel méně estetickou mříž. Dveře z chodby 17 na schodiště musí mít dle požadavků na kolaudaci minimální požární odolnost EW 30 a musí být vybaveny zavíračem, jelikož právě tyto dveře budou oddělovat od sebe požární úseky. Jako kování na dveře na schodiště doporučuji dveřní kování s oboustrannou koulí. To v kombinaci se zavíračem eliminuje možnost lidské chyby (opomenutí zamknout tyto dveře). Toto potlačí jak únik hostů bez placení či vynášení aktiv tímto nehlídaným průchodem, tak i nežádoucí vniknutí do prostoru čajovny ze schodiště, jelikož na schodiště je přes den volný přístup. Podobně dveře do prostoru 19 doporučuji opatřit bezpečnostním kováním s koulí, v tomto případě již postačí jednostranná, opět kvůli opomenutí zamknout. Zde postačí kování Rostex 802
- Použití jednoduchého kamerového systému pro kontrolu chodby 01 a zároveň části chodby 17, tudy totiž předpokládám pohyb pachatele v objektu. Bude zároveň působit jako dohledový aparát nad příchozími a odchozími hosty. Zároveň poslouží v případě nedovoleného vniknutí do objektu jako důkazní materiál pro policejní orgány. Sestavu bude tvořit jedna kamera namířená na vchodové dveře, umístění je zaznačeno v půdorysu . Dále kabel s koncovkami pro připojení DVR zařízení, které bude umístěno v horním patře budovy mimo prostor čajovny. To z toho důvodu, že pachatel nebude moci sabotovat záznam a v případě požáru nebude záznam poničen ohněm ani hasebním zásahem a může tak sloužit k identifikaci místa vzniku požáru, případně odhalení žháře. DVR volíme se čtyřmi vstupy pro případ, kdyby majitel chtěl systém rozšířit (například o střežení svého bytu či okolí domu, což se v budoucnu předpokládá), 4 kamery by pro podobný objekt měly být naprosto dostačující. Kapacita disku 250 giga plnně dostačuje. Monitorovaný prostor musí být samozřejmě vybaven cedulkou informující zákazníky o skutečnosti, že je monitorován. Je též samozřejmě nutné vyřešit právní podmínky a získat povolení

úřadu pro ochranu osobních údajů, jelikož kamera bude snímky ukládat. Celková cena je sice vyšší, avšak vzhledem k zájmům, které ochraňuje, je adekvátní.

- Režimová opatření – především důsledné zavírání dveří od skladu, opomenutí zamknutí řeší kování – koule. Zavírání dveří na schodiště je zabezpečeno zavíračem, kterým dveře musí být vybaveny podle požadavků HZS.
- Nasazení fyzické ostrahy považuji za naprosto zbytečné, neekonomické a především nevhodné kvůli charakteru objektu. Tuto roli bude částečně plnit běžný personál podniku.

Majitel hodlá prostor čajovny v budoucnu pojistit, jeví se tedy moudré zřídit tato opatření i z důvodu, že by se tím snížilo placené pojistné. Z uvedeného vyplývá, že je nutné provést bezpečnostní posouzení objektu ve smyslu ČSN CLC/TS 50131-7.

5.6.1 Bezpečnostní posouzení objektu

Druhy aktiv v objektu, zejména tabáky, čaje a vodní dýmky jsou poměrně atraktivní a snadno zpeněžitelné a lehce přenosné atributy, ztrátu při vykradení objektu odhaduji na 20.000,- Kč, vzhledem k pořizovací ceně PZTS, je to hraniční hodnota, avšak v budoucnu plánuje majitel rozšířit systém hlídání i na byt, který se nachází nad čajovnou, pak by bylo možné využít stávající ústředny a náklady by již nebyly tak vysoké. Historie krádeží v objektu je zatím nulová, vzhledem k tomu, že dosud není v provozu. Vandalismus a žhářství v okolí objektu nejsou časté. Velká okna jsou starší, lehce překonatelná, malá jsou nová, avšak svým rozměrem nepřekračují 900 cm^2 proto není nutné opatřovat je detektory otevření, starší větší okna však bude nutné osadit mřížemi. Do objektu bude mít po zprovoznění samozřejmě přístup veřejnost, již nyní má přístup na schodiště 12, jelikož se jedná o bytový dům a vchod je přes den otevřen. Po otevření provozu bude čajovna fungovat zhruba od 14:00 do 22:00 hod. Držitelem klíčů od objektu bude pouze majitel a personál. Objekt je obklopen ostatními obytnými domy a kriminalita v oblasti není nijak vysoká, dojezdový čas SBS nebo policie je do 10 minut. Stávající zabezpečení je v podstatě nulové, kromě běžných zámků chybí i MZS. Kromě požárních předpisů rozebraných výše nejsou na objekt uplatňovány žádné jiné předpisy ovlivňující PZTS. Z hlediska nasazení detektorů počítáme pouze s PIR a magnetickými kontakty, pro tyto detektory jsem nenalezl v objektu žádná omezení, stejně jako jiné rušivé vlivy uvnitř objektu. Vlivy působící vně objektu také neznamenají v našem případě žádná omezení,

jelikož především světová orientace objektu (vliv paprsků slunce) je pro nasazení PZTS velmi výhodná. Stupeň zabezpečení stanovuji na druhý, jelikož v objektu nejsou skladovány předměty značné hodnoty, není tedy nutné chránit objekt vyšším stupněm podle pravidla, že cena opatření by neměla překročit možnou škodu způsobenou realizací hrozeb.

Pro realizaci navrhuji použít již zmíněný bezdrátový systém Jablotron JA-6x. bude vybaven jednou venkovní sirénou se světelnou signalizací. Návrh umístění bezpečnostních prvků je zakreslen červeně v plánu v Příloze 88.

5.7 Ekonomická rozvaha

Vzhledem k faktu, že čajovna dosud není v provozu, zavádíme do rozvahy pouze předpokládanou tržbu.

součty		51733			60000	**8267**
položka rozvahy		-			+	
číslo	položka	cena	počet	výsledná cena		
CCTV						
1	kamera	890	1	890		
2	dvr	3590	1	3590		
3	kabel	315	1	315		
4	konektory	34	1	34		
5	sata disk	1350	1	1350		
PZTS						
6	ústředna JA-63KR	3520	1	3520		
7	magnetické kontakty	1004	5	5020		
9	PIR	1292	5	6460		
10	klávesnice	1376	1	1376		
11	siréna	2629	1	2629		
EPS						
12	hlásiče	805	6	4830		
MZS						
13	kování ROSTEX koule/koule	2 322	1	2 322		
14	kování ROSTEX 802	949	1	949		
15	mříže		5	20770		
16	tržby za 1. měsíc				20000	
17	tržby za 2. měsíc				20000	
18	tržby za 3. měsíc				20000	

Tabulka 13 Ceník pro navrhované komponenty

Zdroj vlastní

Z uvedeného vyplývá, že při předpokládaných výdělcích z provozu čajovny 20000 korun měsíčně, bude majitel schopen zaplatit všechna bezpečnostní opatření až po třech měsících provozu. Doporučuji proto postupnou realizaci, která by začala EPS a pokračovala MZS, jelikož to jsou největší slabiny objektu, poté je teprve vhodné řešit další aspekty zabezpečení.

Cena za provedení analýzy je:

Počet hodin	Sazba za hodinu	Celkem Kč
14	500	7000

Tabulka 14 Ocenění analytické činnosti

Zdroj vlastní

ZÁVĚR

V průběhu zpracování DP jsem dospěl ke konstatování, že bezpečnostní analýza je velmi široký pojem a lze ji realizovat mnoha různými způsoby. V teoretické části jsem rozebral nejčastější model bezpečnostní analýzy v kapitole 2. U jednotlivých metod jsem však zjistil mnohdy výrazné odlišnosti od tohoto modelu, ty závisí na charakteru zkoumaného objektu, u některých typů analýz, například u checklistu, strukturu z kapitoly 2 dokonce naprosto vypouštíme. Je tedy na osobě analytika, jak se s tímto problémem vypořádá a kterou metodu pro danou situaci zvolí. Toto rozhodnutí je vhodné učinit na základě zkušeností z praxe, většinou je však stanoveno, pro jakou situaci či typ podniku se která analýza hodí nejlépe. Při samotném zpracování analýzy se pak projeví analytikovi schopnosti a nadání pro tuto práci, nemalý dopad na výsledek bude mít i v úvodu zmíněný bezpečnostní čich.

V praktické části jsem navrhnul komplexní ochranu objektu dle přání majitele (což lze považovat za bezpečnostní politiku, byť nezpracovanou písemně). Dle zásad komplexnosti bylo využito několik typů protiopatření, tedy pro zpomalení průniku v podobě MZS, preventivní v podobě kamery a hlásičů požáru a PZTS a také režimová opatření. Kombinací těchto ochran získáme solidní zabezpečení objektu proti všem zjištěným rizikům.

Analýza, jako základní kámen pro tvorbu jakýchkoliv rozhodnutí je jedním z pilířů oboru bezpečnosti, bez jejího přínosu bychom nikdy nedokázali plnně využít nejnovějších technických opatření a jejich efekt by tak nedosáhl zamýšlené úrovně. Je proto nutná pečlivost a odbornost při její tvorbě a soustavné vzdělávání v oboru, jelikož i zde se objevují nové trendy, postupy a inovace.

ZÁVĚR V ANGLIČTINĚ

During the processing of this document, I came to find that security analysis is a very broad term and can be implemented in many different ways. In the theoretical part, I disassembled the most common model of safety analysis in Chapter 2. For each method, however, I often find significant differences from this model, which depends on the nature of the investigated object, for some types of analysis, such as a checklist, the structure of Chapter 2 is even totally different. It is therefore the analyst job, how to deal with this problem and which method will he choose for the situation. This decision should be made on the basis of practical experience, usually it is recommended for what situation or type of business is analysis best suited for. In the very process of analysis is then shown the analyst's ability and aptitude for the job, also "security smell" will have a great effect.

In the practical part I have proposed a comprehensive protection of the building according to the owner (which can be considered a security policy, even when it is not written). According to the principles of complexity has been used several types of countermeasures, thus slowing the penetration in the form of bariers, preventive as cameras and fire alarms and electronic security and regime measures. By combining these protections we get a solid protection of property against all identified risks.

Analysis, as the cornerstone for any decision making is one of the pillars of the security profession, without its benefit we could never fully use the latest technological developments and their impact would not reach the intended level. It is therefore necessary to be patient and educated if we want to process security analysis. It is also necessary to continue education in this field, since even here there are new trends, innovations and practices.

SEZNAM POUŽITÉ LITERATURY

Tištěné materiály:

[1] BRABEC, F. a kol.: *Bezpečnost pro firmu, úřad, občana*. Public History, Praha 2001. ISBN 8086445046

[2] BRABEC, F. a kol. *Ochrana bezpečnosti podniku*. Eurounion Praha, 1996. ISBN 8085858290.

[3] ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. [s.l.] : [s.n.], 2009. 134 s. ISBN 978-80-7399-731-1.

[4] KŘEČEK, Stanislav: *Příručka zabezpečovací techniky*. Crisetus 2002. ISBN 80-902938-2-4.

[5] LAUCKÝ, Vladimír: *Technologie komerční bezpečnosti I*. 1. vyd. UTB Zlín 2003. ISBN 80-7318-119-3

[6] LAUCKÝ, Vladimír: *Technologie komerční bezpečnosti II*. 1. vyd. UTB Zlín 2004. ISBN 80-7318-631-9.

[7] LAUCKÝ, Vladimír: *Bezpečnostní futurologie*. UTB Zlín 2007. ISBN 978-80-7318-560-2.

[8] LÁTAL, Ivo, ŠTANTEJSKÝ Michal, *Bezpečnostní zásady ochrany podniků*. GRADA Publishing, 2009. ISBN 80-7175-091-3

[9] *Security magazín*, Praha:FAMily media, s.r.o., r. 2007-2011

[10] SMEJKAL, Vladimír, RAIS Karel, *Řízení rizik ve firmách a jiných organizacích*. GRADA Publishing, 2009. ISBN 978-80-247-3051-6

Interní materiály:

[11] SULOVSKÁ, K. *Bezpečnostní futurologie.* (přednáška) Zlín : UTB FAI, 2010.

[12] VALOUCH, J. *Projektování integrovaných systémů.* (přednáška) Zlín : UTB FAI, 2010.

Internetové zdroje:

[13] *Analýza rizik a havarijní plánování* [online]. 2010 [cit. 2011-05-20]. Dostupný z WWW:

< http://www.hzsmsk.cz/sklad/kraoo/publikace/112_Analyza_rizik_v_HP.doc>.

[14] BABINEC, F. *Management rizika* [online]. Brno : Slezská Universita v Opavě Ústav matematiky, 2005 [cit. 2011-05-20]. Dostupné z WWW: <http://www.math.slu.cz/studmat/AnalyzaRizik/AnalyzaRizik-1.pdf>.

[15] BOŽEK, František ; KOMÁR, Aleš ; MELKES, Vladimír . *army.cz* [online]. 2001 [cit. 2011-04-16]. Řízení rizik ve vojenských objektech . Dostupné z WWW: <http://www.army.cz/avis/vojenske_rozhledy/2001_2/115.htm>.

[16] *Breaking Down the FMEA* [online]. 2009 [cit. 2011-05-20]. Dostupné z WWW: < http://gcaptain.com/breaking-fmea?10929>.

[17] CIMICKÝ, Jan . Modelování v oblasti řízení rizika . In *5. mezinárodní konference Řízení a modelování finančních rizik* [online]. Ostrava : VŠB-TU Ostrava, Ekonomická fakulta, katedra Financí, 2010 [cit. 2011-05-20]. Dostupné z WWW: <http://www.ekf.vsb.cz/miranda2/export/sites-root/ekf/konference/cs/okruhy/archiv/rmfr/prispevky/dokumenty/Cimicky.Jan_1.pdf>

[18] *CPQRA* [online]. 2010 [cit. 2011-05-20]. Dostupný z WWW:

< ftp://ftp.feq.ufu.br/Luis/Seguran%E7a/Safety/GUIDELINES_Chemical_Process_Quantitative_Risk_Analysis/0720X_07.pdf>.

[19] ČERMÁK., Miroslav. *Clever and smart* [online]. 2008 [cit. 2011-04-16]. Dostupné z WWW: <http://www.cleverandsmart.cz/>.

[20] *Encyklopedie BOZP* [online]. 2009 [cit. 2011-04-16]. HAZOP. Dostupné z WWW: <http://web.vubp-praha.cz/wiki/index.php/HAZOP>.

[21] *ETA* [online]. 2010 [cit. 2011-05-20]. Dostupný z WWW:

< www.theiet.org/factfiles/health/hsb26b.cfm?type=pdf>.

[22] *FMEA* [online]. 2010 [cit. 2011-05-20]. Dostupný z WWW:

< http://www.theiet.org/factfiles/health/hsb26a.cfm?type=pdf>.

[23] *FTA* [online]. 2010 [cit. 2011-05-20]. Dostupný z WWW:

< www.theiet.org/factfiles/health/hsb26c.cfm?type=pdf>.

[24] *Jablotron* [online]. 2009 [cit. 2011-05-09]. Poplachové systémy. Dostupné z WWW: < http://www.jablotron.cz/upload/File/pnj131-2007.pdf >.

[25] *Modelování v oblasti řízení rizika* [online]. 2010 [cit. 2011-05-20]. Dostupný z WWW: < http://www.ekf.vsb.cz/miranda2/export/sites-root/ekf/konference/cs/okruhy/archiv/rmfr/prispevky/dokumenty/Cimicky.Jan_1.pdf>.

[26] PASSEROVÁ, Helena. *Bpm-tema.blogspot.com* [online]. 2007 [cit. 2011-05-20]. Rizika a procesy - úvod. Dostupné z WWW: <http://bpm-tema.blogspot.com/2007/11/rizika-procesy-vod.html>.

[27] *PHA* [online]. 2010 [cit. 2011-05-20]. Dostupný z WWW:

< www.ntnu.no/ross/slides/pha.pdf>.

[28] *Přehled metodik pro analýzu rizik* [online]. 2010 [cit. 2011-05-20]. Dostupný z WWW:

< http://aplikace.mvcr.cz/archiv2008/hasici/planovani/metodiky/mzprakp.pdf>.

[29] *Safety audit checklist* [online]. 2010 [cit. 2011-05-20]. Dostupný z WWW:

< http://www.google.cz/url?sa=t&source=web&cd=1&sqi=2&ved=0CBsQFjAA&url=http%3A%2F%2Fwww-ppd.fnal.gov%2Feshbmgoffice-w%2FESH%2520Management%2FSafety_Audit_Checklist_Guide%2520v0.3.doc&rct=j&q=Safety%20audit%20checklist&ei=S4fWTezSPM3ysgb95sCYBw&usg=AFQjCNF3K4LGufwOiP_NVm-HkUcXFpjAhA&cad=rja

>.

[30] *SWOT analýza* [online]. 2010 [cit. 2011-05-20]. Dostupný z WWW:

< www.kvic.cz/showFile.asp?ID=2097>.

[31] *SWOT* [online]. 2010 [cit. 2011-05-20]. Dostupný z WWW:

<http://halek.info/prezentace/planovani-organizovani-prednasky/poprp-print.php?l=02>.

[32] TABAS, Marek ; BABINEC, František ; LÁSKOVÁ, Andrea . *Odborné časopisy* [online]. 2006 [cit. 2011-04-16]. Význam analýzy metodou HAZOP při tvorbě

bezpečnostní dokumentace . Dostupné z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=31467>.

[33] *Think tank* [online]. 2010 [cit. 2011-05-20]. Dostupný z WWW:

< http://standupforamerica.files.wordpress.com/2009/11/think-tank.jpg >.

[34] *Velaction.com* [online]. 2010 [cit. 2011-05-20]. What's Good for the Goose ISN'T Good for the Gander. Dostupné z WWW: <http://www.velaction.com/leading-change-checklists/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GottaGoLean+%28Gotta+Go+Lean+Blog+by+Jeff+Hajek%29>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACCESS	Systém pro kontrolu vstupu
BA	Bezpečnostní analýza
DP	Diplomová práce
EM	Elektormagnetický
EPS	Elektronická požární signalizace
HZS	Hasičský záchranný sbor
IT	Informační technologie
MZS	Mechanické zábranné systémy
PC	Stolní počítač
PCO	Pult centralizované ochrany
PČR	Policie české republiky
PIR	Pasivní infračervený detektor pohybu
PTZS	Poplachové, tísňové a zabezpečovací systémy
UI	Utajované informace

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: CHECKLIST PRO BEZPEČNOSTNÍ AUDIT PŘÍLOHA

Požární a bezpečnostní zařízení	**Ano**	**Ne**	**Neznámé**
Je správné požární a bezpečnostní zařízení k dispozici?	☐	☐	☐
Je zařízení přístupné (tj. je odblokováno)?	☐	☐	☐
Jsou hořlaviny uložené v tomu odpovídajících skříních?	☐	☐	☐
Provoz strojů nebo složitých zařízení			
Jsou kontrolky na přístroji v OK nebo bezpečném stavu?	☐	☐	☐
Produkuje zařízení běžné zvuky, pachy a výsledky?	☐	☐	☐
Je přístroj vybavených záznamníky údajů nebo monitory, které sledují stav zařízení?	☐	☐	☐
Pokud je to nutné, existují protokoly údržby nebo jiné záznamy, které sledují stav zařízení?	☐	☐	☐
Byly někdy odzkoušeny techniky lockout/tagout?	☐	☐	☐
Běžné nástroje a vybavení			
Používají zaměstnanci správné nástroje pro svou práci?	☐	☐	☐
Používají zaměstnanci své nástroje správným způsobem?	☐	☐	☐
Pokud je to nutné, byli zaměstnanci vyškoleni k použití určitých nástrojů?	☐	☐	☐
Jsou nástroje v dobré a bezpečné kondici?	☐	☐	☐
Byly nástroje v poslední době zkontrolovány?	☐	☐	☐
Jsou nástroje uloženy ve vhodných místech?	☐	☐	☐
Pracovní prostor a údržba			
Má pracovní prostor čistý vzhled?	☐	☐	☐
Jsou všechny uličky a průchody dostatečně široké pro personál a pohyb zařízení?	☐	☐	☐
Mají všechny uličky používané pro pohyblivé zařízení přímou viditelnost?	☐	☐	☐
Mají všechny pochozí/pracovní plochy stěny nebo držadla na ochranu zaměstnanců před nebezpečím?	☐	☐	☐
Jsou chemické látky správně inventarizované a skladované odděleně?	☐	☐	☐
Je osvětlení adekvátní?	☐	☐	☐
Jsou východy jasně označeny a snadno k nalezení?	☐	☐	☐
Jsou zajištěny veškeré režijní položky?	☐	☐	☐
Jsou všechny schody v dobrém a bezpečném stavu?	☐	☐	☐
Jsou všechny žebříky řádně zajištěny, nebo skladovány odděleně?	☐	☐	☐
Je celková stavba v dobrém stavu?	☐	☐	☐
Obecné postupy			
Mají personál a návštěvníci budovy znalosti o evakuačních postupech při požáru či jiné MU?	☐	☐	☐
Mají návštěvníci laboratoří osobu uvnitř oraganizace, která je koordinuje?	☐	☐	☐
Je si manažer oddělení dostatečně vědom prací provedených návštěvníky laboratoří nebo zaměstnanci z jiných oddělení?	☐	☐	☐
Personální Ergonomie, vzdělávání a prostředky osobní ochrany			
Pracují zaměstnanci způsobem, který je bez zbytečné fyzické námahy?	☐	☐	☐
Vykonávající pracovníci odpovídající ergonomii?	☐	☐	☐
Jsou pracovníci dostatečně zaměřeni na jejich práci, zejména v případě, kde je určité nebezpečí?	☐	☐	☐
Jsou pracovníci vyškoleni pro práci a jsou si vědomi rizika a procedur k jeho snížení?	☐	☐	☐
Zdá se být práce vhodný pro personal, který ji vykonává?	☐	☐	☐
Pokud je to nutné, používají pracovníci prostředky osobní ochrany?	☐	☐	☐
Pro práci v blízkosti strojů, jsou pracovníci vybaveni odpovídajícím oblečením?	☐	☐	☐
Pokud je to nutné, jsou zaměstnanci vybaveni TLD dozimetry v ozářených oblastech?	☐	☐	☐

P II: DOKUMENT PRO POSOUZENÍ OBJEKTU

Objekt: .....

Stanovení stupně zabezpečení : **1 2 3** Třída klasifikace prostředí : **I II III IV**

Typ objektu :

Rodinný dům ☐	Chata, Chalupa ☐	Garáž ☐
Byt činžovní ☐	Byt – panelák ☐	Byt v rodinném domě ☐
Kanceláře ☐	Obchod ☐	Výrobní prostory ☐

Umístění střežených prostor:

Suterén ☐	Přízemí ☐	1. Patro ☐
2. Patro ☐	3. Patro a vyšší ☐	Podkroví ☐

Konstrukce objektu:

Zděný ☐	Prefabrikát ☐	Mont. ocelová hala ☐
Dřevěná roubenka ☐	UNIMO dřevěný ☐	UNIMO ocelový ☐
Dřevený – panel ☐		

Konstrukce vnitřní:

Zděný ☐	Smíšený ☐	Dřevěná roubenka ☐
Prefabrikát ☐	Sádrokarton ☐	Dřevěný panel ☐

Konstrukce střechy:

Štítová 90° ☐	Štítová 120° ☐	Rovná ☐
Břidlice ☐	Tašky ☐	Plech rovný ☐
Eternit ☐	Došky ☐	Plech vlnitý ☐

Kritická místa:

Okna ☐	Hlavní dveře ☐	Zadní dveře ☐
Světlík ☐	Střešní okno ☐	

Poloha objektu:

Řadová zástavba ☐	O samotě stojící ☐	Mírně svažitý terén ☐
Do 100 m ☐	Rovný terén ☐	Prudký svah ☐

Historie vloupání:

1 x ročně ☐	Vícekrát ročně ☐	Dosud nevloupáno ☐

Speciální požadavky:

Detektor kouře ☐	Detektor plynu ☐	Záplavový detektor ☐

Při poplachu zasahuje:

Majitel ☐	Agentura PCO ☐	Policie ČR ☐
Soused ☐	Hlídací agentura ☐	Městská policie ☐

Reakce na poplach:

Do 5 minut ☐	Do 15 minut ☐	Více než 30 minut ☐

Rušivé vlivy vnitřní:

Ventilace, vzduchotech ☐	Netěsnosti oken a dveří ☐	Zářivky, halog. Osvětlení ☐

Rušivé vlivy vnější:

Výtahy, el.motory ☐	Vysílače AM, FM,TV, GSM ☐	Těžká doprava,tramvaje ☐

Zvláštní opatření, poznámky :

Závěr : Datum : .....

....

dodavatel objednatel

PŘÍLOHA P III: PŮDORYS ANALYZOVANÉHO OBJEKTU