

Analýza ochrany majetku firmy PEDST

Jiří Sochor

Bakalářská práce
2014



Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav krizového řízení

akademický rok: 2013/2014

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Jiří Sochor**
Osobní číslo: **L11102**
Studijní program: **B3909 Procesní inženýrství**
Studijní obor: **Ovládání rizik**
Forma studia: **prezenční**

Téma práce: **Analýza ochrany majetku firmy PEDST**

Zásady pro vypracování:

1. Zpracování literární rešerše zaměřené na analýzu ochrany majetku firmy PEDST.
2. Posouzení současného stavu bezpečnosti a ochrany majetku firmy s důrazem na prvky obvodové a plášťové ochrany.
3. Analýza vybraných bezpečnostních rizik, které ohrožují majetek firmy PEDST.
4. Návrh na redukci vybraných rizik, které mají vliv na zabezpečení majetku firmy PEDST.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] LUKÁŠ, Luděk a kolektiv. **Bezpečnostní technologie, systémy a management I.** Zlín: Radim Bačuvčík ? VeRBum, 2011, ISBN 978-80-87500-05-7.

[2] LUKÁŠ, Luděk a kolektiv. **Bezpečnostní technologie, systémy a management II.** Zlín: Radim Bačuvčík ? VeRBum, 2012, ISBN 978-80-87500-19-4.

[3] ŠEFČÍK, Vladimír. **Analýza rizik.** Zlín: Univerzita Tomáše Bati, 2009, ISBN 978-80-7318-696.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **doc. Ing. Miroslav Tomek, Ph.D.**

Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **21. února 2014**

Termín odevzdání bakalářské práce: **9. května 2014**

V Uherském Hradišti dne 21. února 2014


prof. PhDr. Ivo Barteček, CSc.
děkan




doc. PhDr. Ferdinand Mazal, CSc.
ředitel ústavu

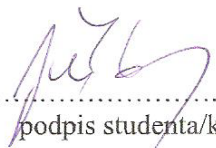
Prohlašuji, že

- beru na vědomí, že odevzdáním 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 předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v archivu Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji 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 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 – 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval/a samostatně a použitou literaturu jsem citoval/a. V případě publikace výsledků budu uveden/a jako spoluautor/ka
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Uherském Hradišti dne 28. 4. 2014


.....
podpis studenta/ky

ABSTRAKT

SOCHOR, Jiří. *Analýza ochrany majetku firmy PEDST*. [Bakalářská práce]. Univerzita Tomáše Bati ve Zlíně. Fakulta logistiky a krizového řízení. Ústav krizového řízení. Vedoucí: doc. Ing. Miroslav Tomek, Ph.D. Stupeň odborné kvalifikace: Bakalář (Bc.). Studijní program: Procesní inženýrství, studijní obor: Ovládání rizik. Zlín: FLKŘ UTB, 2014, 54 s.

Předmětem bakalářské práce je literární rešerše analyzování ochrany majetku firmy PEDST. V praktické části jsou popsány jednotlivé druhy zabezpečení a jejich analyzování. Cílem práce bylo analyzovat vybraná bezpečnostní rizika a návrh na redukci vybraných bezpečnostních rizik ve firmě PEDST.

Klíčová slova: Analýza, bezpečnost, ochrana, podnik, riziko

ABSTRACT

SOCHOR, Jiří. *Analysis of the protection of company assets PEDST*. [Bachelor thesis]. Tomas Bata University in Zlin. Faculty of Logistics and Crisis Management. Institute of crisis management. Supervisor: doc. Ing. Miroslav Tomek, Ph.D. Level of professional qualifications: Bachelor (Bc). Study program: Process Engineering Study: Risk Control. Zlín: FLKŘ UTB, 2014, p 54.

Subject of the thesis is a literature review analyzing the protection of company assets PEDST. The practical part describes the different kinds of security and their analysis. The aim of the study was to analyze a security risk and a proposal for reducing certain security risks in the company PEDST.

Keywords: Analysis, security, safety, enterprise risk

Poděkování

Tímto bych chtěl poděkovat zejména vedoucímu mé bakalářské práce panu doc. Ing. Miroslavu Tomkovi, Ph.D. za jeho poskytnuté odborné rady, ochotu a čas při konzultacích. Dále bych chtěl poděkovat panu Milanu Nedůchalovi a panu Ing. Pavlu Vašíčkovi za jejich vstřícnost a poskytnuté informace, bez kterých by nebylo možné tuto práci dokončit a rodině a blízkým za jejich podporu při studiu.

OBSAH

ÚVOD	7
I TEORETICKÁ ČÁST	8
1 MAJETEK PODNIKU PEDST A JEHO OCHRANA	9
2 BEZPEČNOSTNÍ ANALÝZA PODNIKU PEDST	14
II PRAKTICKÁ ČÁST	25
3 POSOUZENÍ SOUČASNÉHO STAVU ZABEZPEČENÍ PODNIKU PEDST	26
3.1 ZABEZPEČENÍ U JEDNOTLIVÝCH KATEGORIÍ BUDOV V PODNIKU PEDST	27
3.2 ZABEZPEČENÍ AREÁLU PODNIKU PEDST	32
4 ANALÝZA VYBRANÝCH BEZPEČNOSTNÍCH RIZIK V PODNIKU PEDST	35
4.1 SEMIKVANTITATIVNÍ HODNOCENÍ RIZIKA V PODNIKU PEDST	36
4.2 METODA „PNH“	38
4.3 VYHODNOCENÍ RIZIK V PODNIKU PEDST- METODA „PNH“	40
5 NÁVRH NA REDUKCI VYBRANÝCH BEZPEČNOSTNÍCH RIZIK V PODNIKU PEDST	41
ZÁVĚR	48
SEZNAM POUŽITÉ LITERATURY	49
SEZNAM OBRÁZKŮ	51
SEZNAM TABULEK	52
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	53

ÚVOD

„Je potřeba zajistit maximální možnou ochranu“ nebo „udělejte to tak, aby se do objektu nikdo nedostal“. Tyto a další podobné fráze můžeme dnes slyšet od manažerů firem stále častěji a častěji. A taky se není čemu divit. V dnešní, rychle se měnící době, kdy technologie a výpočetní technika jdou mílovými kroky stále dopředu, se najde i mnoho takových, kteří, ať už z jakéhokoli důvodu, nejsou spokojeni se svou stávající situací a rozhodnou se řešit své problémy po svém. Dalo by se říci, že počty kriminálních činností, zaměřených převážně na majetkové trestné činy rok od roku stoupají. Také samotná vloupání do velkých objektů jsou čím dál častější a pachatelé pro svou činnost využívají stále důmyslnějších a modernějších postupů a zařízení. Díky těmto negativním vlivům si proto mnoho manažerů přeje zajistit maximální ochranu a bezpečnost pro svá aktiva. Ne všichni jsou však ochotni investovat nemalé náklady na instalaci bezpečnostních zařízení či na zajištění ochrany specializovanou bezpečnostní agenturou, a proto se také stávají čím dál častějším cílem nezvaných hostů.

Jedním z nejdůležitějších kroků před samotnou instalací bezpečnostních prvků by měla být včasné a správně provedená bezpečnostní analýza na ochranu majetku, kterou se zabývá v této bakalářské práci. Cílem bakalářské práce je analýza ochrany majetku firmy PEDST. Pro splnění hlavního cíle, jsem si stanovil tyto dílčí cíle, kterými jsou posouzení současného stavu zabezpečení podniku PEDST a analýza vybraných bezpečnostních rizik a jejich redukce. Pro zpracování bakalářské práce jsem si zvolil metody analýzy, syntézy, sběru dat, indukci a dedukci. Tuto práci jsem rozdělil do dvou hlavních částí.

V první části se zabývám teoretickým výkladem analýzy pro ochranu majetku ve firmě, včetně zmínění jednotlivých prvků potřebných k zajištění bezpečnosti.

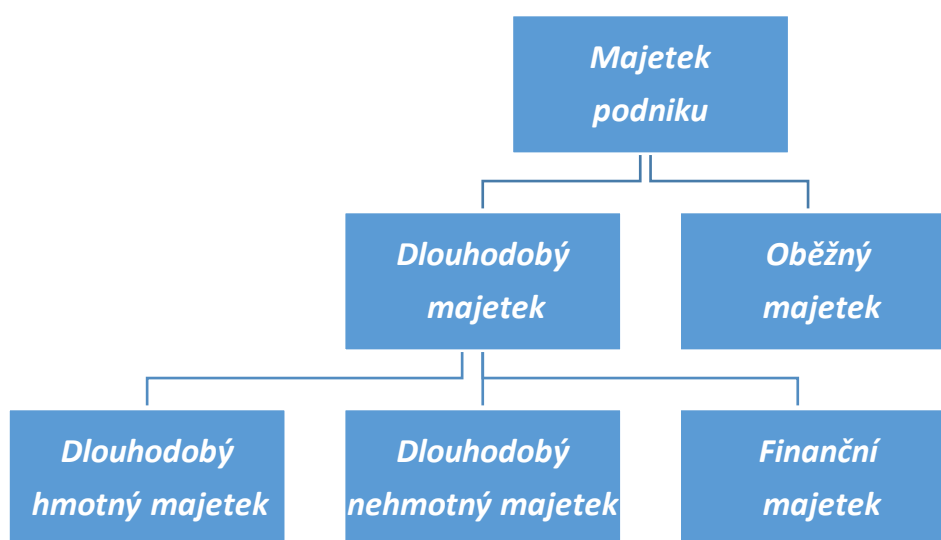
V druhé části je realizována praktická studie, ve které posuzuji současný stav bezpečnosti a ochrany majetku firmy s důrazem na prvky obvodové a plášťové ochrany.

I. TEORETICKÁ ČÁST

1 MAJETEK PODNIKU PEDST A JEHO OCHRANA

Pro zajištění správného chodu podniku a úspěšnost samotné podnikatelské činnosti, je potřeba vybavit se takovým majetkem, který odpovídá právě konkrétnímu typu podnikání. Je třeba také rozlišovat původ majetku, zda byl do podnikání vložen či získán jinými zákonnými způsoby.[18]

Druhy majetku se člení podle doby jeho užívání a podle výše pořizovací ceny. Grafické rozdělení na obrázku (1) pojednává o druzích majetku, které mohou být zastoupeny v podniku. [18]



Obrázek 1- Druhy majetku v podniku[Zdroj: 18]

U podnikající fyzické osoby (dále jen pFO), se za obchodní majetek považuje majetek, který jí patří a který slouží nebo je určen k podnikání.

U právnické osoby (dále jen PO), se obchodním majetkem rozumí veškerý majetek evidovaný v účetnictví.

Dlouhodobým hmotným majetkem se rozumí majetek s dobou používání delší než jeden rok a pořizovací cenou vyšší než 40000,- Kč.Jedná se o:

- výrobní linky,
- stavby,
- automobily,
- pozemky,
- stroje a zařízení.

Dlouhodobý nehmotný majetek je majetek, u nějž je doba používání delší než jeden rok a pořizovací cena překročí částku 60 000,- Kč. [18]Dlouhodobým nehmotným majetkem může být:

- software,
- licence,
- patenty,
- know-how.

U finančního dlouhodobého majetku, mluvíme převážně o majetek v podobě dlouhodobých cenných papírů, u nichž není stanovena minimální cena, ale jejich doba držení překračuje dobu jednoho roku.Dlouhodobým finančním majetkem mohou být [11]:

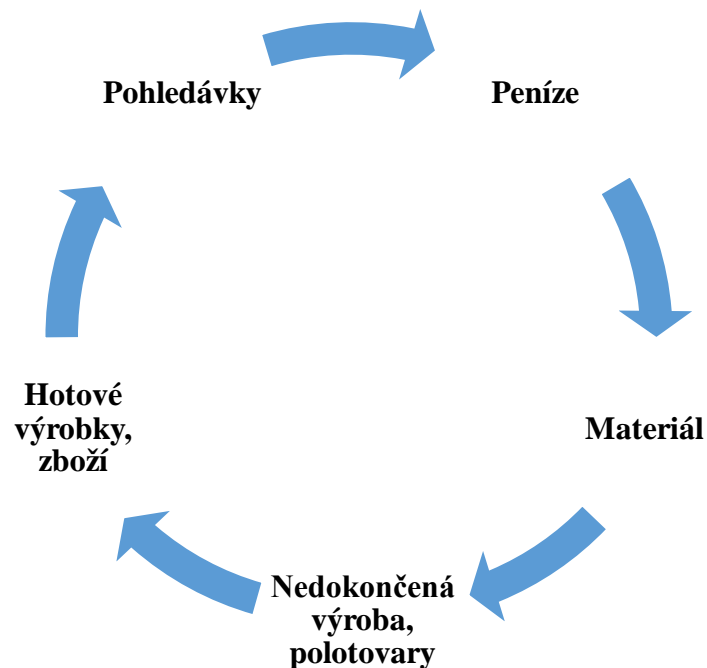
- akcie,
- obligace,
- vklady.

Do drobného hmotného a nehmotného majetku,spadá takové vybavení firmy, které svou dobou použitelnosti splňuje podmínku pro stanovení dlouhodobého majetku, ale cena tohoto majetku nepřekračuje částku 40 000,- Kč resp. 60 000,- Kč. [18]Příklady drobného hmotného a nehmotného majetku:

- kopírka 5000,- Kč,
- nábytek 25 000,- Kč,
- sekačka 10 000,- Kč.

Oběžným majetkem, jako na obrázku (2) se rozumí majetek, jehož doba používání ve firmě nepřekračuje dobu jednoho roku a zároveň pořizovací cena není vyšší než 40000,- Kč za jednotku. [18] Příklady oběžného majetku:

- zásoby,
- krátkodobý finanční majetek,
- peněžní prostředky,
- pohledávky.



Obrázek 2- Znárodnění oběžného majetku v podniku[Zdroj: 18]

Jednotlivé druhy majetku jsou součástí podniku a zajišťují jeho správný chod a konkurenceschopnost. Každý z těchto jednotlivých majetků se může stát potenciálním cílem nežádoucích návštěvníků, a proto je potřeba klást důraz na jeho zabezpečení a ochranu proti zneužití, odcizením, zničením, apod., *Ochrana v obecném pojetí představuje vytvoření bezpečného prostředí pro daný subjekt. Realizace ochrany představuje návrh a sladění všech dostupných prostředků, které zajistí požadovanou nebo definovanou bezpečnost.* [16] Bezpečnost je stav, ve kterém jsou na akceptovatelnou úroveň eliminována rizika plynoucí z hrozeb. Má-li být subjektu zajištěna bezpečnost, musí být dobře známy základní hrozby, které mu mohou způsobit újmu. Mezi základní hrozby v současné době patří činnosti kriminálních živlů či jiných osob, jejichž cílem bývá zcizení majetku, neoprávněné nakládání s ním nebo úplné poškození či zničení chráněných aktiv. Způsob provedení hrozby či její naplnění určují opatření, jimiž je zajištěna ochrana proti takovýmto účinkům. Jednotlivá bezpečnostní opatření, která by se měla v podniku nacházet a která bývají realizovaná ve formě systému fyzické bezpečnosti, jsou schopna potenciálního narušitele odradit od jeho úmyslu, zamezit provedení činu nebo zpomalit jeho postup při zcizení aktiv.

Režimová opatření podniku jsou opatření, která představují procesní naplnění bezpečnostní politiky organizace. Cílem těchto opatření je stanovit zásady, pravidla a oprávnění při

pohybu zaměstnanců či dalších osob v prostorách organizace. Režimová opatření stanovují způsoby nakládání s bezpečnostně důležitými prvky, pravidla provádění bezpečnostních kontrol vnášeného a vynášeného materiálu či nakládání s bezpečnostními materiály, apod. Režimová opatření by měla být navrhována způsobem, který by bral ohled na zaměstnance podniku a příliš neomezoval pohyb osob v prostorách organizace. Současně však musí být navržena tak, aby zajišťovala požadovaný stupeň bezpečnosti. Významnou úlohu v této oblasti zastává systém kontroly vstupu (tzv. přístupový systém).

Kindl o režimové ochraně uvádí: „Režimová ochrana je souborem organizačně administrativních opatření a postupů směřujících k zajištění požadovaných podmínek pro smysluplnou funkci zabezpečovacího systému a jeho sladění s provozem chráněného objektu.“ [16]

Ochranná opatření uplatňovaná na chráněném pozemku podnikutvoří aplikaci takových procesů či bezpečnostních prvků v podniku, které mají za úkol odradit potenciální pachatele a zpomalit či zamezit jejich dalšímu postupu v páchání trestné činnosti. Jedná se o prvky perimetrické ochrany, plášťové ochrany, prostorové ochrany a předmětové ochrany.

Perimetrickou nebo i obvodovou ochranou rozumíme souhrn takových bezpečnostních opatření, která jsou uplatňována na obvodu chráněného objektu (pozemku, parcely) a v prostoru mezi hranicí pozemku a chráněným objektem. *„Perimetrem je jeho katastrální hranice, která bývá vymezena přírodními nebo umělými bariérami.“ [16]* Perimetrická ochrana by měla zajistit signalizování, pokud by došlo k poškození nebo překročení obvodu objektu. K takovéto signalizaci je zapotřebí využít senzory pro vnější použití, které mají vyšší odolnost proti vniknutí prachu, nečistot a vody do přístroje. Problémem venkovního zabezpečení však může být velké množství faktorů podněcujících senzor k signalizaci narušení objektu (např. zvěř, pohyb rostlin, vítr, apod.). Tyto systémy se nejčastěji kombinují s tzv. CCTV systémy (ClosedCircuitTelevisionSystem). Pro ochranu perimetru se používají nejčastěji např. mikrovlnné bariéry, infračervené závory, laserové závory, zemní tlakové hadice, apod.

Hovoříme-li o plášťové ochraně, hovoříme tak o souhrnu bezpečnostních opatření fyzické bezpečnosti realizovaných na plášti a vedoucích k zajištění chráněného objektu, zpravidla budovy. Plášťová ochrana je zpravidla tvořena zdmi, dveřmi, zámky, okny, mřížemi, bezpečnostními fóliemi, apod. Cílem ochrany je nejen zajistit bezpečnost chráněných aktiv

uvnitř budovy, ale také zamezit jakémukoliv nežádoucímu průniku do těchto prostor. Plášťová ochrana slouží také jako prostředek k odstrašení narušitele, znemožnění průchodu či zbrzdění postupu pachatele a jeho odhalení. [16]

Do plášťové ochrany se řadí také prvky elektronické bezpečnostní signalizace, kterými jsou zejména kamerové systémy, vnitřní a venkovní detekční systémy, detektory narušení plášťové ochrany, apod. Cílem prostorové ochrany je zajistit odhalení pohybu pachatele uvnitř chráněné budovy a jeho zpomalení v následném postupu.

Prvky prostorové ochrany bývají instalovány zpravidla uvnitř chráněných budov, a to zejména na chodbách, schodištích či v jednotlivých místnostech. Pro zabezpečení prostorové ochrany se používají dveře, zámky, mříže, kamerové a detekční systémy, poplachové zabezpečovací systémy a systémy kontroly vstupu. V rámci prostorové ochrany by měly detekční systémy narušení prostoru signalizovat vniknutí do vnitřních prostor chráněného objektu.

Předmětová ochrana je tvořena opatřeními, která vedou k zamezení nebo minimalizaci možností zcizení chráněných aktiv a neoprávněné nakládání s nimi. Za chráněná aktiva můžeme považovat cenné umělecké předměty, cenné fyzické předměty, patentově chráněné vzory či další z jakéhokoli důvodu pro nás cenné předměty, apod. Předmětovou ochranu tvoří zejména skříně, vitríny, skleněné tabule, poplachové a kamerové systémy nebo systémy sloužící pro detekci neoprávněného vniknutí do chráněného prostoru či k námi střeženému zájmu. Detektory narušení by měli poukázat na bezprostřední přítomnost narušitele u námi chráněného zájmu a na jakoukoliv manipulaci s takto chráněným předmětem. Detektory narušení, které jsou určeny převážně k monitorování přítomnosti narušitele, mívají zpravidla širokoúhlou a plochou detekční charakteristiku a krátký dosah. [16]

„Je neefektivní vynakládat na bezpečnostní opatření náklady, které převyšují samotnou hodnotu chráněných aktiv, proto by úroveň jednotlivých ochran měla odpovídat hodnotě chráněných aktiv a stupni zabezpečení.“ [16] Před jakoukoliv implementací bezpečnostních prvků měla být řádně provedena bezpečnostní analýza v podniku.

2 BEZPEČNOSTNÍ ANALÝZA PODNIKU PEDST

Bezpečnostní analýza (dále jen BA), je souhrn postupů a metod aplikovaný na jednotlivých vrstvách objektu za účelem zjistit možné slabiny či bezpečnostní díry v podniku. Cílem BA je identifikovat maximum možných zranitelných míst či nedostatků, které mohou být obsaženy ve zkoumaném objektu, odhadnout hrozby, rizika a jejich možné negativní dopady na zkoumaný objekt. BA nám také může pomoci určit míru efektivity a funkčnosti stávajících bezpečnostních prvků a navrhnout tak řešení pro zlepšení či zvýšení efektivity tak, aby byla pokryta a snížena všechna možná rizika na akceptovatelnou úroveň.[1]

Hovoříme-li o bezpečnostní analýze, mluvíme tak o určité metodě zkoumání, při níž se provádí dekompozice (rozklad) objektu na tzv. základní prvky. Při provádění BA se vyhledává a zkoumá vnitřní zranitelnost podniku, vnější hrozby a implementované (aplikované) mechanismy, které působí nebo mohou působit na jednotlivé prvky ve zvolených vrstvách bezpečnosti[28]:

- personální,
- fyzické,
- organizační,
- administrativní,
- komunikační,
- počítačové.

Existuje velké množství metod, podle kterých by mohla být prováděna bezpečnostní analýza podniku. Rozdělení těchto metod a jejich stručná identifikace je uvedena v tabulce (1).

Kvalitativní metody	Kvantitativní metody
rychlejší a jednodušší	exaktní metody
subjektivní vliv	časově náročné
kvalifikovaný odhad	formalizované postupy
pracující s daty o možných následcích a ztrátách	1. krok- pravděpodobnost výskytu jevu
využití kontextů	2. krok- pravděpodobnost ztráty
stanovují míry ohrožení a zranitelnosti	důraz na dostupnost a spolehlivost vstupních dat

Tabulka 1- Rozdělení metod bezpečnostní analýzy[Zdroj: 28]

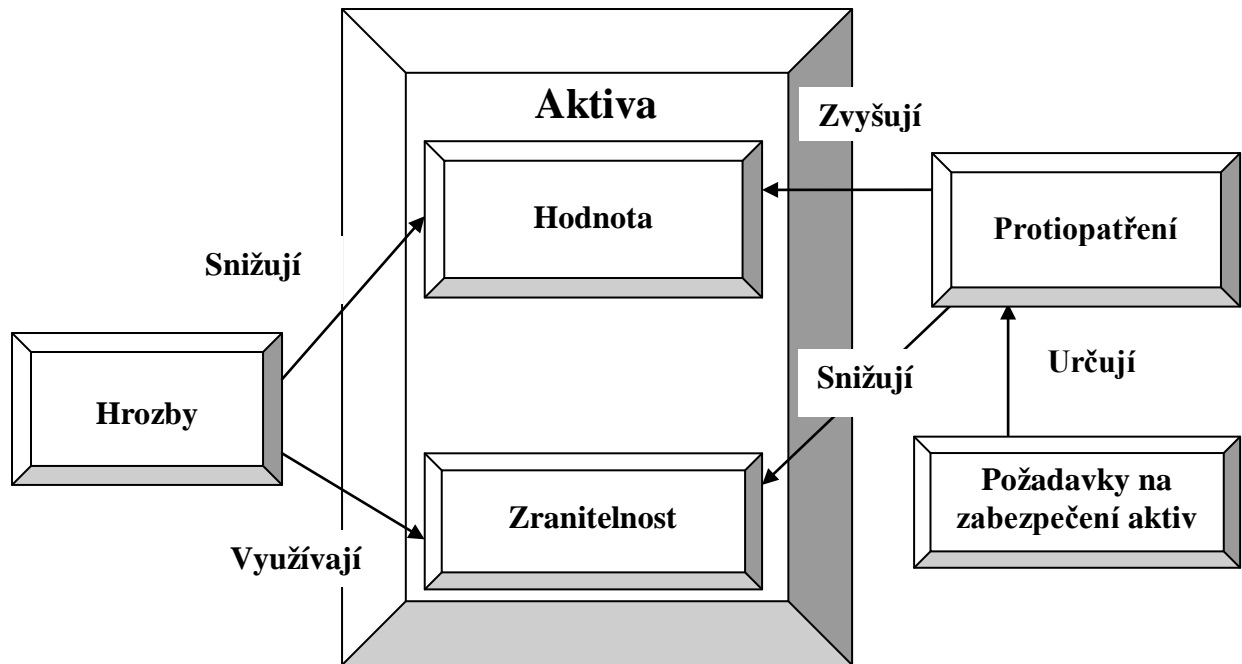
V tabulce (2) jsou znázorněny hrozby, které mohou mít dopad na objekt či organizaci,

Řešení bezpečnosti				
Hrozby		Objekt, organizace	Protiopatření	
Poruchy	Přírodní kalamita		Bezpečnost informačního systému	Organizační opatření
Internet	Požár		Bezpečnost práce	Požární ochrana
Epidemie	Špionáž		Řízení rizik	Personální politika
Konkurence	Úrazy		Audity	Školení
Zaměstnanci	Selhání informačního systému		Politika	Pojištění
Legislativa	Zásobování			Fyzická bezpečnost
Terorismus	Kriminalita			

včetně protiopatření, která mohou minimalizovat popř. odvrátit jejich dopad.

Tabulka 2- Řešení bezpečnostních rizik v organizaci [Zdroj: 28]

Hrozba jako taková, představuje jakýsi protiklad od příležitosti. Hrozbou pro podnik může být příliv nové a silné konkurence, ekonomická situace ve státě, velké výkyvy počasí či ztráta dobrého jména, apod. Na obrázku (3) jsou znázorněny vzájemné vztahy mezi hrozbou, aktivem, protiopatřením a zranitelností podniku. Aby bylo možné bezpečnostní rizika systematicky redukovat, je nutné zavést určitá opatření či procesy, které tomu napomohou. V tomto kroku je potřeba nalézt možná hrozící rizika. Při hledání rizik by se mělo vycházet z oblastí, které jsou nejbližší k danému „projektu“ (např. projekt stavebnictví či výstavby výškových budov bude mít jiné oblasti rizik než např. bezpečnostní agentura). Zároveň je potřeba sledovat, zda nebyly zavrhnuty tzv. „jistá rizika“. Jestliže existuje předpoklad, že se něco s určitostí přihodí, nejedná se o riziko, neboť v tomto případě je nejistota kompletně odstraněna. Ve fázi identifikace rizik je vhodné přizpůsobit samotné hledání rizik tak, aby nedošlo k zahlcení velkým množstvím nalezených rizik. Čím bude snaha o nalezení rizik větší, tím více jich bude také nalezeno. [21]



Obrázek 3- Vzájemné vztahy mezi hrozbou, protiopatřením, aktivem a zranitelností [Zdroj: 28]

„Jestliže (ne)můžeme riziko měřit, (ne)můžeme je řídit.“

Analýzou bezpečnostních rizik zjišťujeme míru hrozícího rizika a také jeho dopad a potenciální ztráty. Při analýze rizik je důležité použít vhodnou metriku, které zúčastnění rozumí. Využití kvalitní metriky (nízké, střední, vysoké riziko) je snadnější pro komunikaci s projektovým týmem. Kvantitativní metrika (5 dnů, 1000 Kč, 5 bloků, atd.) je vhodná pro interní kontrolu projektu nebo pro jednání s klientem.[21]

Proces analýzy rizik můžeme rozdělit do následujících etap:

- **identifikace aktiv:** vymezení posuzovaného subjektu a popis aktiv, která podnik vlastní,
- **stanovení hodnoty aktiv:** určení hodnoty a význam aktiv pro podnik, ohodnocení možného dopadu jejich ztráty, změny či poškození na existenci či chování podniku,
- **identifikace hrozeb a slabin:** určení druhů událostí a akcí, které mohou negativně ovlivnit hodnotu aktiv, určení slabých míst podniku, které mohou umožnit působení hrozeb,
- **stanovení závažnosti hrozeb a míry zranitelnosti:** určení pravděpodobnosti výskytu hrozby a míry zranitelnosti podniku vůči dané hrozbě.[28]

Při analýze hrozeb a zranitelností se berou v úvahu realizovaná protipatření, která mohou mít za následek snížení úrovně hrozby a zranitelnosti s využitím např. Semikvantitativního hodnocení a analýzy rizik metodou „PNH“.

Realizace různých druhů hrozeb v podniku může mít za následek celou řadu negativních dopadů, jak na jednotlivé složky nacházející se v podniku, tak na podnik celkově.

Dopady finančního charakteru (nebo jen finanční dopady), jsou negativní dopady vzniklé působením nežádoucí situace na organizaci. Takovými dopady mohou být obvykle finanční ztráty, pokles zisku, zvýšení nákladů, apod. Číselná velikost finančních dopadů, které jsou přiřazeny jednotlivým stupňům ohodnocení, se bude lišit v závislosti na finanční síle podniku (pro menší podniky může být ztráta v řádu milionů korun kritická, zatímco pro větší podniky nemusí takováto ztráta nutně způsobit výrazné finanční problémy).[10]

Při realizaci výskytu určitých druhů rizik, nemusí mnohdy jejich dopady vést pouze k finančním ztrátám, ale často jsou spojeny s negativními dopady nefinanční povahy. Mezi nejvýznamnějšími jsou např. dopady na lidské zdraví, životy, kulturní dědictví, bezpečnost, životní prostředí či dopady sociálního charakteru nebo poškození dobrého jména, apod.[10]

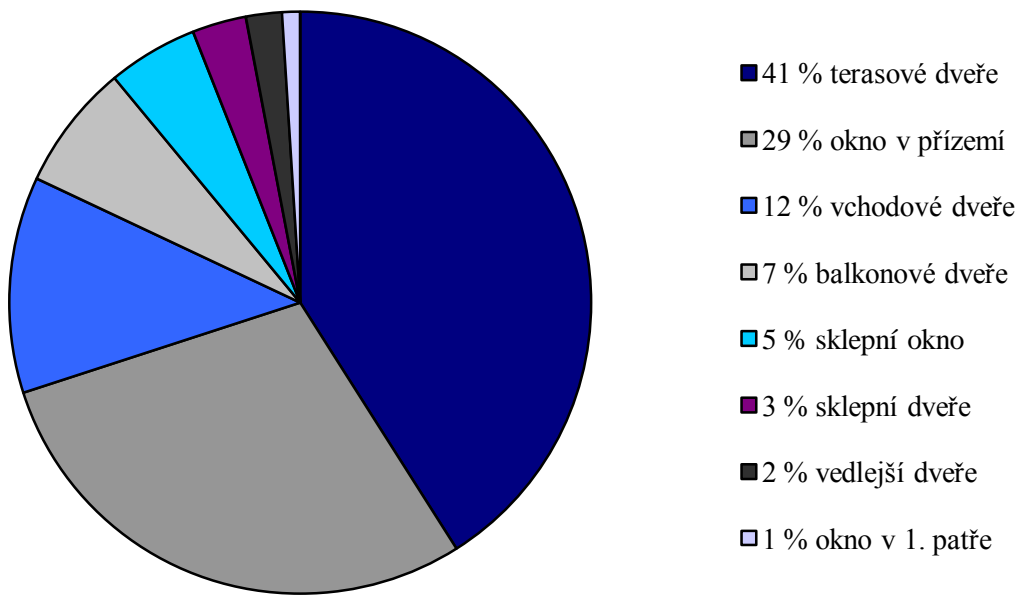
I když bývá riziko obvykle spojeno s jeho negativními dopady, neměla by se jeho analýza omezit pouze na tuto stránku, ale měla by věnovat pozornost i na pozitivní stránku spojenou s novými příležitostmi. K ohodnocení tohoto typu rizik je možné pak přistupovat stejně, jako hodnocení negativní stránky. V tabulce(3) jsou uvedeny příklady stupnic měření finančních dopadů. Je zřejmé, že specifikace stupnic měření finančních dopadů jsou nezbytným předpokladem operacionalizace stupnic hodnocení dopadů.[10]

Stupeň hodnocení	Pokles zisku		Vzrůst investičních nákladů v (%)
	Stupnice A (USD)	Stupnice B (Kč)	
Nevýznamný	< 10 tis.	< 5 mil.	< 5
Nízký	10 tis. - 100 tis.	5 mil. - 20 mil.	5 - 10
Střední	100 tis. - 1 mil.	20 mil. - 50 mil.	10 - 15
Vysoký	1 mil. - 10 mil.	50 mil. - 100 mil.	15 - 30

Tabulka 3- Stupnice měření poklesu zisku a vzrůstu investičních nákladů[Zdroj: 10]

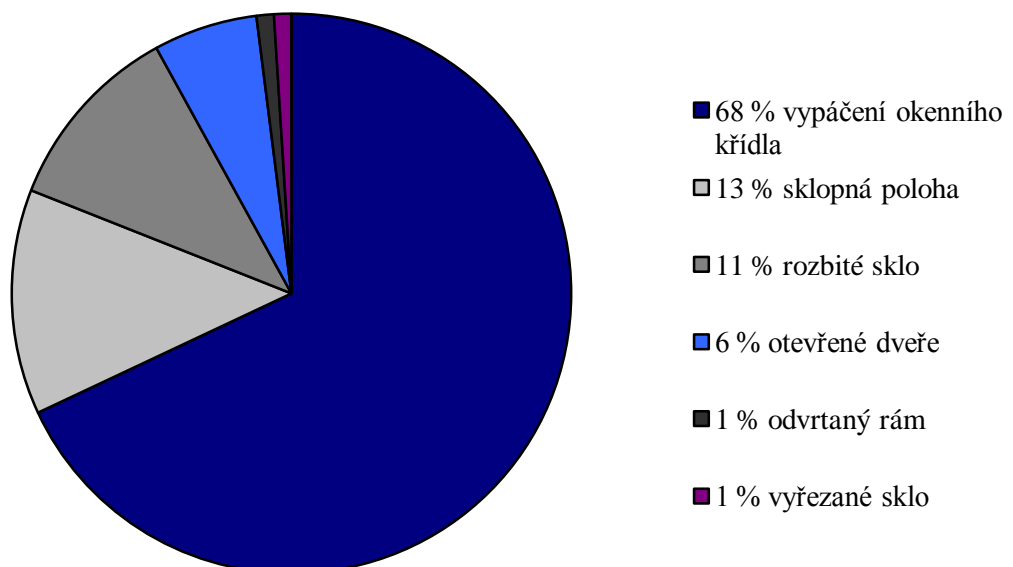
Pro hodnocení rizik můžeme použít nejrůznější postupy a metody, univerzální návod žádný zákon neudává. Ať už se rozhodnete použít jakoukoliv metodu, nejdůležitější je, aby přinesla použitelné a užitečné výsledky. [21]

Krokem prioritizace rizik se rozumí hledání takových rizik, která jsou důležitá a mají podstatný dopad na „projekt“. Do tohoto kroku řízení rizik se výborně hodí tzv. „Paretovo pravidlo 80/20“, které nám ukazuje poměr vynaloženého úsilí a konečného výsledku snažení (20% našeho úsilí nám přináší 80% výsledků, ale také naopak 80% vynaloženého úsilí nám může přinést v důsledku pouze 20% výsledků). Jestliže budeme ohodnocovat rizika kvantitativně, můžeme prohlásit za nejdůležitější ta, u kterých víme, že jejich realizace by měla pro nás nejhorší dopad. Tato rizika mají nejvyšší hodnotu. Při plánování řízení rizik navrhujeme jednotlivé postupy vedoucí k jejich minimalizaci. Uvádíme zde také, kdo bude za takový postup zodpovědný a do kdy se postup realizuje. V moderních postupech jsou do vyhodnocení zahrnovány také příčiny rizik, které stojí za pravděpodobnostivzniku rizika a jeho dopadu na projekt. Monitorování rizik je důležité zdůvodu vyřazení rizik, která již nejsou na seznamu důležitých rizik a nastartování opětovného procesu identifikace nových rizik. [21] Výše hrozícího rizika závisí na specifických situacích a vyplývá z hodnoty chráněného aktiva, úrovně hrozby a zranitelnosti aktiva. Při provádění analýzy rizik se pracuje s veličinami, které není možné v mnoha případech přesně změřit a určení jejich velikosti spočívá mnohdy na kvalifikovaném odhadu specialisty, jenž se vyjadřuje na základě svých zkušeností. [28] V grafech (1 a 2) jsou procentuálně vyjádřeny hodnoty vniků pachatelů do objektu.



Graf 1- Použití nejčastějších vniků pachatelů do objektu [Zdroj: 28]

Z uvedených údajů na grafu (1) můžeme snadno vyčíst, že 82% pachatelů použila pro vniknutí objektu okna a terasové dveře, nikoliv však vchodové. Existuje 70% případů, kdy lupiči vypáčili okna velmi snadno a tiše obyčejným šroubovákem.



Graf 2- Použití nejčastějších metod vloupání pachatelů [Zdroj: 28]

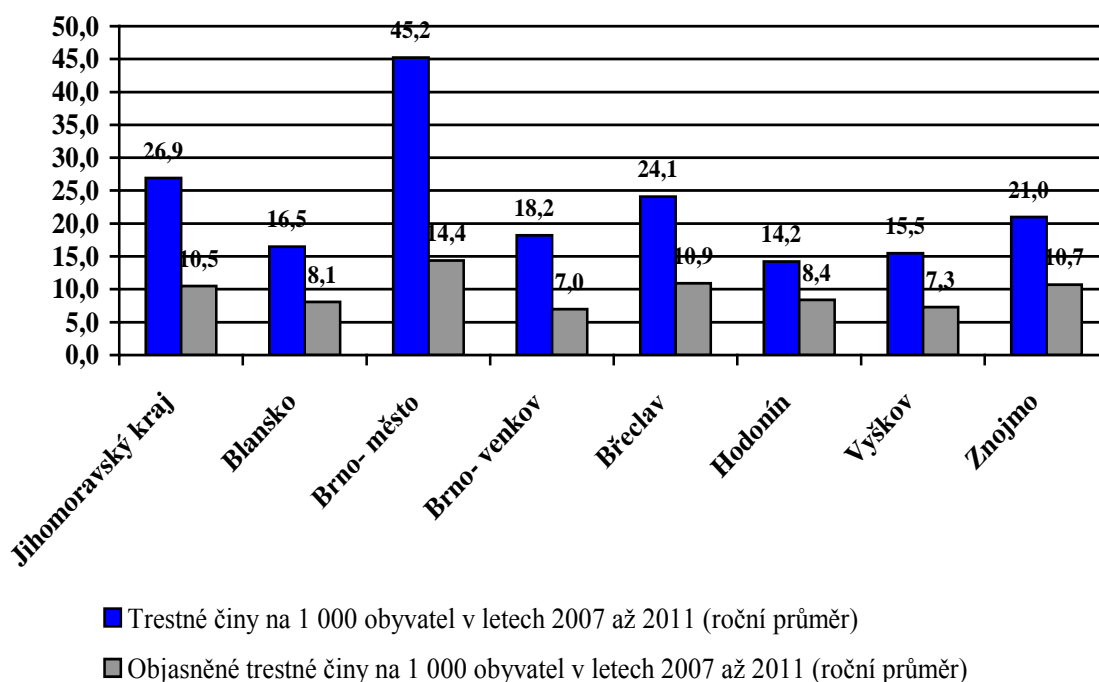
V grafu (2), můžeme vidět nejčastější postupy při vloupávání do objektů. Většina vloupání, ke kterým došlo, se odehrávala mezi 12:00-20:00 hodinou.

V tabulce(4) jsou uvedeny druhy trestních činnů včetně počtů trestních činů v jednotlivých okresech Jihomoravského kraje za rok 2013. Pro účely práce je zvýrazněn okres, na který se analýza ochrany majetku firmy vztahuje.

	Zjištěné		z toho						Objasněné trestné činy
	celkem	index 2013/ 2012	obecné činy	z toho				hospodářské činy	
				násilné činy	krádeže vloupáním	krádeže prosté	ostatní majetkové činy		
Kraj celkem	15 608	102,9	12 297	976	2 761	5 785	1 088	1 644	5 267
v tom okresy:									
Blansko + Vyškov	1 409	90,8	1 023	107	336	302	122	136	606
Brno - město	8 733	109,8	7 190	391	1 276	4 082	621	931	2 356
Hodonín	1 124	90,9	790	126	192	234	67	140	556
Břeclav	1 280	103,9	960	94	239	385	74	140	562
Znojmo	1 229	95,3	850	134	222	237	100	163	569

Tabulka 4- Kriminalita v Jihomoravském kraji a jeho okresech v roce 2013 [Zdroj: 15]

V grafu (3) je zobrazena četnost spáchaných trestných činů a objasněných trestných činů v Jihomoravském kraji za období 2007-2011 na 1 000 obyvatel.



Graf3- Trestné činy zjištěné a objasněné na 1 000 obyvatel v okresech Jihomoravského kraje v letech 2007 až 2011 (roční průměry)[Zdroj: 14]

V rámci zajištění fyzické bezpečnosti, zahrnují bezpečnostní situace široké spektrum událostí. Adekvátní reakce vyžadují určené a speciálně připravené osoby, které jsou schopné zajistit bezpečnost jimi chráněných aktiv efektivní cestou a s minimálními možnými dopady. Fyzická ostraha podniku, která zajišťuje samotnou fyzickou ochranu objektu, plní v této oblasti významnou roli.

Svojí přítomností v objektu organizace je FO schopna, v souladu s režimovými opatřeními, zajistit ochranu aktiv. Svojí činností se zasazuje především o odhalení a zadržení narušitele, realizaci protipožárních opatření, realizaci havarijních opatření či zamezení zcizení aktiv, apod. Fyzická ostraha může být prováděna jak hlídači či policisty, tak i specializovanou hlídacím službou.

Většina organizací pro zajištění své fyzické ochrany využívá služby poskytované jinými právními subjekty, zpravidla soukromými bezpečnostními agenturami. Zajišťování fyzické ochrany ostrahou bývá, po finanční stránce, nejnákladnější způsob vedoucí k zajištění ochrany a bezpečnosti.[16]

Technické prostředky ochrany podniku představují současně s fyzickou ostrahou základní bezpečnostní opatření fyzické bezpečnosti objektu. Cílem technických bezpečnostních

prostředků je podpořit realizaci režimových opatření, zkvalitňovat činnosti fyzické ostrahy, odradit narušitele od jeho činu, případně významně ztížit jeho činnost a prodloužit tak dobu pro přístup k chráněným zájmům.

Mezi základní technické prostředky zajišťující fyzickou ochranu objektu patří různé druhy mechanických zábranných systémů či elektronických bezpečnostních systémů. [16]

V tabulce (5) je znázorněn přehled českých technických norem pro aplikaci mechanických zábranných systémů

Označení normy	Předmět normy
ČSN P ENV 1627-1630	Dveře, okna, uzávěry - Odolnost proti násilnému vniknutí
ČSN EN 1906	Stavební kování - Dveřní štíty, kliky a knoflíky
ČSN EN 12320	Stavební kování - Visací zámky a příslušenství
ČSN EN 13126-1	Stavební kování - Okna a balkonové dveře
ČSN EN 1155	Stavební kování - Elektricky poháněná zařízení a otevírače dveří
ČSN 74 7731	Dveře odolnější proti vloupání
ČSN 949	Okna, dveře - stanovení odolnosti proti nárazu měkkým a těžkým tělesem
ČSN 16 5190	Stavební kování - Cylindrické vložky
ČSN EN 1522	Okna, dveře, uzávěry a rolety - odolnost proti průstřelu
ČSN EN 1303	Cylindrické vložky pro zámky
ČSN EN 1300	Bezpečnostní úschovné objekty - Zámky s vysokou bezpečností
ČSN EN 1143-1	Bezpečnostní úschovné objekty

Tabulka 5- Přehled českých technických norem [Zdroj: 27]

Kvalitativní schopnosti činnosti narušitele vyjadřují jeho znalosti, dovednosti a technické vybavení, jimiž disponuje při překonávání systému fyzické bezpečnosti.[16]

V praxi se určují čtyři stupně zabezpečení, jež se odvíjí od hodnoty objektu, který je potřeba zabezpečit a určitého předpokladu úrovně znalostí možného narušitele:

- 1. stupeň zabezpečení, „**nízké riziko**“ je vhodný pro objekty s nízkým předpokladem vniku narušitele. Jedná se především o garáže, byty, chaty, rodinné domy, strojovny, apod. Tento stupeň zabezpečení předpokládá, že možní pachatelé

disponují pouze omezenými znalostmi o poplachových zabezpečovacích systémech a mají omezený sortiment snadno dostupných nástrojů;

- U 2. stupeň zabezpečení, „**nízké až střední riziko**“, se předpokládá, že znalosti pachatelů týkající se poplachových zabezpečovacích systémů jsou omezené a pachatelé pro svůj čin použijí běžné nářadí či přenosné systémy (např. multimetr). Teno stupeň zabezpečení je vhodný např. pro komerční objekty;
- 3. stupeň zabezpečení, „**střední až vysoké riziko**“ předpokládá, že možní narušitelé objektu jsou obeznámeni s poplachovými zabezpečovacími systémy a pro spáchání činu mají k dispozici rozsáhlý sortiment nástrojů a přenosných elektrických zařízení. Zabezpečení 3. stupně se využívá zejména u objektů, ve kterých se nacházejí zbraně, ceniny, narkotika, informace, apod;
- 4. stupeň, „**vysoké riziko**“ se používá v případech, kdy má zabezpečení prioritu před všemi ostatními hledisky. Předpokládá se, že narušitelé jsou schopni nebo mají možnost zpracovat podrobný plán vniknutí do chráněného objektu a mají k dispozici kompletní sortiment zařízení, včetně prostředků pro náhradu rozhodujících komponentů poplachových zabezpečovacích systémů. Stupeň zabezpečení, s vysokým rizikem vniknutí do objektu, se využívá převážně u objektů národního a vyššího významu. [16]

„Stupeň zabezpečení určuje provedení systému fyzické bezpečnosti, včetně poplachového zabezpečovacího systému a detektorů narušení. Stupeň zabezpečení celého poplachového zabezpečovacího systému je dán nejnižším stupněm zabezpečení kteréhokoliv z použitých komponentů, včetně detektoru narušení.“ [16]

Identifikace opatření tvoří souhrn postupů a metod, které mají za cíl minimalizovat možné riziko na akceptovatelnou úroveň a chránit tak cenná aktiva. [23]

Podle způsobu implementace můžeme jednotlivá opatření rozdělit na:

- **fyzická** kde se jedná o kontrolu pohybu každé osoby, která se nachází ve střežených prostorách. Zabránění průniku neautorizovaných osob do zabezpečených prostor;
- **administrativní** opatření provádějící se za pomoci procedur, standardů, politiky a směrnic, které definují určitá závazná pravidla a postupy. Do administrativního opatření můžeme dále zařadit aktivity, jako jsou např. řízení rizik či školení v oblasti bezpečnosti;

- **logická** opatření, sloužící k řízení a vyhodnocování přístupu k informačním zdrojům prostřednictvím autorizací, autentizací, identifikací, odpovědnosti uživatele, apod.:
 - systémová: specifické nastavení na úrovni operačního systému,
 - aplikační: specifické nastavení na úrovni aplikace,
 - databázová: specifické nastavení na úrovni databáze,
 - komunikační: specifické nastavení aktivních síťových prvků,
 - preventivní: měly by útočníkovi zabránit v realizaci jeho úmyslu a tím předcházet nežádoucím aktivitám,
 - detekční: slouží pro odhalení nežádoucí aktivity např. senzorem, analýzou záznamů z kamer a logů,
 - nápravná: cílem je zabránit opakování dané události např. změnou stávajícího procesu,
 - odstrašující: tato opatření by měla být viditelná, aby útočníka odradila od nežádoucího jednání,
 - zdržující: opatření, která by měla postup útočníka co nejvíce zpomalit, aby mohla být jeho aktivita detekována,
 - reaktivní: poté co je nežádoucí aktivita odhalena, je nutné na ni nějakým způsobem reagovat, reakce může být ofenzivní nebo defenzivní,
 - obnova: opatření slouží k obnově funkčnosti systému. [23]

II. PRAKTICKÁ ČÁST

3 POSOUZENÍ SOUČASNÉHO STAVU ZABEZPEČENÍ PODNIKU PEDST

Areál podniku PEDST zobrazen na obrázku (4), se nachází v průmyslové zóně ve Strážnici v těsné blízkosti hlavního silničního tahu Břeclav – Zlín.

Areál o celkové výměře 55 800 m² je tvořen pěti hlavními přízemními halami a jednou pěti podlažní skladovací budovou, dále dvou podlažní administrativní budovou, vrátnicí, objekty pro pomocné provozy, parkovacími místy (+ přístřešek pro jízdní kola), manipulačními, zpevněnými a zelenými plochami. Areál je kompletně oplocen a zajištěn ostrahou bezpečnostní agentury (včetně obsluhy vstupu – vrátnice). V současnosti slouží areál podniku k pronájmu ostatním firmám, které prostory využívají převážně pro skladové účely. Obsazení areálu není jednotvárné, jedná se o různé druhy firem počínaje od dřevozpracujících podniků přes stavební materiály a sklářský průmysl až po vinařství.



Obrázek 4- Areál podniku [Zdroj: vlastní]

Ze zadní části sousedí areál s podnikem, kterým byl v nedávné době odkoupen. Ze zbylých stran je areál obklopen komunikacemi, z toho jedním hlavním tahem a dvěma vedlejšími, které slouží jako příjezdové cesty k okolním podnikům. Pro vjezd do areálu je na obvodu vystavena vrátnice s obsluhou v podobě pracovníka soukromé bezpečnostní služby (dále jen SBS). V celkovém areálu je instalováno osvětlení areálu. Nejsou instalována žádná speciální bezpečnostní opatření, včetně kamerového systému.

Pro možnost posouzení aktuálního stavu zabezpečení, ve kterém se podnik PEDST nachází, jsou všechny budovy rozděleny do následujících tří kategorií, a to na:

- **I. kategorie**- skladovací prostory,
- **II. kategorie**- důležité objekty,
- **III. kategorie**- ostatní objekty.

Z důvodu stáří posuzovaných objektů a instalovaných bezpečnostních prvků, jsou pro posouzení současného stavu zabezpečení jednotlivých budov rozděleny aktuální instalované bezpečnostní prvky do dvou úrovní:

- Do **I. úrovně** jsou zahrnuty „klasické“ bezpečnostní prvky, které jsou instalovány samostatně na plášti budovy a takové budovy, které jsou vybaveny pouze těmito základními bezpečnostními prvky, jakými jsou- dřevěná okna, skleněné dveře, plechová vrata, zadlabací či visací zámky;
- Do **II. úrovně** jsou zahrnuty takové budovy, u kterých jsou společně prvky I. úrovně, použity ještě další bezpečnostní prostředky, jako- kamerový systém, bezpečnostní zámky, bezpečnostní kování, bezpečnostní okna, mříže na oknech, kontrola vstupu, závory, turnikety.

3.1 Zabezpečení u jednotlivých kategorií budov v podniku PEDST

Díky různorodosti firem, které se v podniku nyní nachází, jsou každé zjednotlivě obsazených budov jinak zabezpečeny. Všechny posuzované objekty jsou rozděleny do třech kategorií podle jejich charakteru a podle „důležitosti“ objektu pro podnik od nejnižších, což tvoří např. WC, až po prostory jako jsou administrativní stanoviště, atd.:

- **I. kategorie** obsahuje objekty s charakterem skladovacích prostor. Tyto objekty mají v areálu největší zastoupení a díky současnému stavu zabezpečení jsou nejvíce zranitelná;
- **II. kategorie** zahrnuje pro podnik takové objekty, společně prvky vyššího významu, u kterých je kladen vyšší důraz na zabezpečení. Jsou zde zahrnuty objekty jako- vrátnice, administrativní budova, trafostanice, regulační stanice plynu, budova stavebnin;

- **III. kategorie** obsahuje ostatní objekty, které jsou pro podnik méně důležité, nebo takové prvky, na které nejsou kladeny vyšší zabezpečovací nároky, např. sociální zařízení, přístřešek na kola, mostní váha.

Současné zabezpečení objektů I. kategorie

Jak už bylo uvedeno výše, do I. kategorie jsou zařazeny skladovací objekty. Většina skladových prostor plní zabezpečení I. a částečně II. úrovně, kdy se jedná převážně o základní zabezpečení objektu plášťovou ochranou. Nejčastějšími instalovanými prvky na plášti jsou:

- okna s dřevěným orámováním,
- plastová okna,
- plechová vrata,
- zadlabací zámky,
- cylindrické vložky zámků.

Výjimkou může být objekt s označením 19 na obrázku (5), kdy jsou k plášťové ochraně připojeny bezpečnostní prvky II. úrovně. V tomto případě plášťovou ochranu tvoří:

- bezpečnostní plastová okna,
- dřevěná okna doplněna mřížemi,
- bezpečnostní dveře,
- rolety,
- bezpečnostní kování na dveřích,
- kamerový systém.

Současné zabezpečení objektů II. kategorie

Objekty II. kategorie jsou tvořeny převážně objekty, které jsou pro podnik „důležité“ anebo objekty na které jsou kladeny vyšší nároky na zabezpečení. Jedná se např. o administrativní pracoviště, prostory vrátnice či hlavní uzávěry plynu a elektrické energie. Obdobně jako u skladových prostor jsou na plášti instalovány prvky I. i II. úrovně zabezpečení.

Jedná se převážně o:

- dřevěná okna,
- plastová bezpečnostní okna,
- skleněné vchodové dveře,
- bezpečnostní dveře,
- bezpečnostní kování na dveřích,
- zámky s cylindrickými vložkami,
- visací zámky s cylindrickými vložkami.

V případě objektů s označením 31/01 a 36 na obrázku (5) je okolo objektu instalována obvodová ochrana se vstupní bránou.

Současné zabezpečení objektů III. kategorie

Do objektů III. kategorie jsou zahrnuty ostatní objekty nacházející se v areálu. U těchto objektů není potřeba zajišťovat maximální zabezpečení a ochranu. Jedná se o objekty, jako jsou např. WC, přístřešek na kola, vodní nádrž, mostní váha, apod. U těchto objektů se jedná převážně o zabezpečení I. úrovně, kdy jsou k zabezpečení použity nejčastěji:

- plechová vrata s cylindrickou vložkou zámku,
- visací zámky,
- zadlabací zámky,
- dřevěná okna,
- luxferové stěny.

Výjimku tvoří objekt pod označením 2 na obrázku (5), kdy je okolo objektu instalována obvodová ochrana.

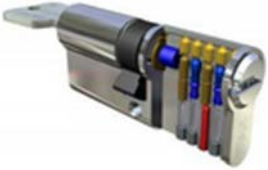




	Charakter objektu	Číslo objektu
	Skladové prostory	05, 06, 10, 11, 13, 15, 18, 19, 26, 27, 28, 32, 33, 35
	Důležité budovy	01, 04, 20, 31, 36
	Ostatní objekty	02, 03, 07, 08, 14, 16, 17, 21, 22, 23, 24, 25, 29, 34, 38

Obrázek 5- Situační plánec podniku [Zdroj: vlastní]

Jelikož, je v areálu podniku PEDST různé zastoupení firem s různým odvětvím podnikání, je také jiné zabezpečení jednotlivých objektů. V I. kategorii, kdy se jedná převážně

o skladové prostory je nejčastěji používaným zabezpečovacím prostředkem zámeček s cylindrickou vložkou či zadlabací zámeček. Jako vhodné prvky pro eliminaci tohoto rizika, a zvýšení úrovně zabezpečení, je možné použít tzv. bezpečnostní zámky nebo zámky s bezpečnostním kováním jako v tabulce (6), které mají větší průlomovou odolnost.

<p>Bezpečnostní vložka Titan K5 30x35</p> 	<p>Bezpečnostní vložka nejvyšších kvalit s 50 000 různými kombinacemi.</p> <p>Vložka Titan K5 je opatřena niklovým povrchem a neodvratelným tělem.</p> <p>Cena: 660,-Kč s DPH</p>
<p>Stavební vložka Fab 100D 30x35</p> 	<p>Standartní stavební vložka výrobce Fab.</p> <p>Cena: 300,-Kč s DPH</p>
<p>Bezpečnostní kování Vemak V1 72 Cr</p> 	<p>Spolehlivé bezpečnostní kování značky Vemak.</p> <p>Toto kování na dveře je osazeno bezpečnostní kovanou krytkou vložky.</p> <p>Cena: 1450,-Kč s DPH</p>

Tabulka 6- Prvky pro zabezpečení vchodových dveří [Zdroj:9]

Pro zabezpečení objektů II. kategorie, do které spadají převážně objekty administrativní budovy a vrátnice, je v současné době využito převážně cylindrických vložek částečně v kombinaci s bezpečnostním kováním. Jako možný doplněk pro zvýšení bezpečnosti lze provést instalaci bezpečnostních kamer jako na obrázku (12). Bezpečnostní kamery je možné využít i pro posílení zabezpečení objektů III. kategorie, kdy se jedná např. o místo k parkování kol a mopedů, které je v současné době prakticky nestřeženo.

3.2 Zabezpečení areálu podniku PEDST

Po celém obvodu areálu podniku PEDST jsou instalovány prvky obvodové ochrany, jakými jsou převážně ploty a zdi. Vchod do areálu je střežen pomocí SBS a pracovníka ostrahy (dále jen POs), který sídlí v prostorách vrátnice. Po celém areálu podniku PEDST jsou instalovány světla veřejného osvětlení. Bezpečnostní firma, kterou si podnik PEDST pronajímá pro zajištění ochrany pro svá aktiva, působí na trhu již od roku 1995. Její hlavní specializací je, mimo jiné, práce v oblasti zajišťování ochrany pro velké podniky, kdy na základě provedení bezpečnostní analýzy a individuálních potřeb zákazníků, jsou navrhovány nejlepší způsoby pro zajištění bezpečnosti. Mezi hlavní služby poskytované SBS je zajišťování fyzické ostrahy objektů, poskytování služeb pomocí pultu centrální ochrany, ochrana osob a majetku, apod.

Vrátnice nacházející se v podniku PEDST je integrována do obvodové ochrany a slouží k monitorování a evidenci vozidel, které vjíždí a vyjíždí z areálu. Zároveň slouží vrátnice jako stanoviště pro pracovníky soukromé bezpečnostní služby.

Povinnosti a oprávnění pracovníka ostrahy:

- zajišťovat evidenci a monitoring vozidel, kontrolu osob,
- kontrola zabezpečení proti vniknutí třetích osob do místa ostrahy s výjimkou osob vedených v seznamu oprávněných osob,
- plnit funkci ohlašovny požáru,
- dodržovat platné předpisy BOZP a PO.

Časové obsazení pracovníka ostrahy:

- denní směna: (So+Ne) 06:00 – 18:00 hodin – 1 pracovník,
- noční směna: (Po-Ne) 18:00 – 06:00 hodin – 1 pracovník.

Organizace obchůzky:

- obchůzka musí být vykonávána minimálně po dobu 15 minut;
- minimální četnost obchůzek je:
 - pondělí- pátek v době 18:00 – 06:00 2x za směnu,
 - sobota, neděle a svátky v době 18:00 – 06:00 2x za směnu.

Pracovník ostrahy je povinen při vykonávání obchůzky kontrolovat uzamčení a nepoškození vstupů do jednotlivých budov, zajištění a nepoškození oken zpravidla v přízemí, zajištění zaparkovaných vozidel, apod. POs v rámci prevence a mimo dobu stanovených pochůzek po celém areálu, v průběhu celé směny nepravidelně provádí pochůzku po hlavní komunikaci v podniku, a to od vrátnice po objekt stavebnin, a zároveň cestou monitoruje boční prostory.

Pracovník ostrahy monitoruje vjezdy a vstupy do objektu a na základě uvážení je oprávněn kohokoliv zastavit a zeptat se na účel vstupu či vjezdu do areálu podniku PEDST. POs provádí službu tak, aby byl vidět, aby projevoval zájem o to co se v areálu děje a svým chováním a jednáním tak působil jako prevence proti možným nekalým praktikám.

Pomocí metody sběru dat, která byla prováděna při obchůzce po areálu spolu s pracovníkem SBS byly zpozorovány klady a zápory, které mohou mít vliv na zajištění bezpečnosti v podniku PEDST. Mezi hlavní nedostatky týkající se oblasti bezpečnosti, které se v podniku nachází, je možné zařadit chybějící kamerový systém, nízkou bezpečnostní úroveň OO a značné možnosti ukrytí pachatelů související s realizací obchůzky.

Klady:

- osvětlení areálu,
- obvodové ochrana,
- vrátnice,
- bezpečnost areálu zajišťuje SBS,
- účast POs,
- z jedné strany sousedí areál s firmou, kterou byl v nedávné době odkoupen,
- u přední části areálu vede frekventovaná trasa.

Zápory:

- v areálu chybí kamerový systém,
- značné možnosti ukrytí pro potenciální narušitele,
- vrátnice není opatřena závorou,
- ze dvou stran kolem areálu vedou cesty, které jsou v noci málo frekventované,

- nepřítomnost hlídacího psa,
- služba POs pouze od 18:00 do 06:00 hodin,
- obvodová ochrana bez vrcholových zábran,
- snadná překonatelnost obvodové ochrany.

4 ANALÝZA VYBRANÝCH BEZPEČNOSTNÍCH RIZIK V PODNIKU PEDST

V kapitole jsou popsána vybraná bezpečnostní rizika a jejich analýza. Jedním z vybraných bezpečnostních rizik je nedostatečná OO. Na obrázcích (6,7 a 8) je vyobrazen současný stav OO kolem areálu. Konstrukce OO by měla mít za úkol, jak vymezení chráněného území, tak zajištění ochrany území proti vnějším pokusům o vniknutí, a proto by se dalo říct, že současný stav OO může sloužit pouze jako vymezení hranice chráněného objektu, nikoli však jako spolehlivé bezpečnostní opatření.



Obrázek 6- Obvodová ochrana I [Zdroj: vlastní]



Obrázek 7- Obvodová ochrana II [Zdroj: vlastní]



Obrázek 8- Obvodová ochrana III [Zdroj: vlastní]

4.1 Semikvantitativní hodnocení rizika v podniku PEDST

Metoda Semikvantitativního hodnocení spolu s využitím matice rizika slouží k číselnému vyjádření významnosti či faktorů rizik. Při provádění hodnocení je jednotlivým stupňům pravděpodobností výskytu rizik i stupňům intenzity jejich negativních dopadů přiřazováno číselné hodnocení jako v tabulce (7). Ohodnocení významnosti každého rizika je pak stanoveno jako součin ohodnocení pravděpodobnosti, se kterou se riziko vyskytne a ohodnocení negativního dopadu, který by nastal v případě realizace rizika. Pro sestavení číselného ohodnocení pravděpodobností, se kterou se riziko vyskytne, se obvykle volí lineární stupnice, kde je v případě užití pěti stupňů přiřazováno ohodnocení 1, 2, 3, 4, 5. Pro ohodnocení intenzity negativních dopadů se volí stupnice nelineární např. mocninou, kde je ohodnocení daného stupně dvojnásobkem ohodnocení stupně předchozího (1, 2, 4, 8, 16). Z výše uvedené definice vyplývá, že nejméně významným rizikem je riziko s ohodnocením $1 \times 1 = 1$ a naopak nejvýznamnějším je riziko s ohodnocením $5 \times 16 = 80$. Ohodnocení významnosti rizik nabývá tedy hodnot z intervalu 1 – 80. [10]

Hrozící rizika	Pravděpodobnost výskytu rizika	Intenzita negativních dopadů	Ohodnocení rizika
Vniknutí do areálu	5	8	40
Poškození majetku firmy	4	8	32
Závažné poškození majetku firmy spojené s velkými finančními ztrátami	2	16	32
Ztráta majetku firmy	4	8	32
Způsobení zdravotní újmy	3	8	24
Způsobení závažné zdravotní újmy s trvalými následky	2	16	32
Založení požáru	2	16	32
Vyřazení objektu z provozu	2	16	32
Celkové ohodnocení rizik			256

Tabulka 7- Semikvantitativní hodnocení rizika [Zdroj: vlastní]

Semikvantitativní hodnocení významnosti faktorů je možné nyní využít k:

- uspořádání rizik podle významnosti,
- rozčlenění rizik do skupin s různou významností:
 - nejvýznamnější rizika (ohodnocení vyšší než 30),
 - středně významná rizika (od 10 do 30),
 - nejméně významná rizika (nižší než 10),
- stanovení celkového rizika jako součtu ohodnocení významnosti všech rizikových faktorů. [10]

Po aplikaci semikvantitativní analýzy na možná hrozící rizika v podniku bylo zjištěno, že do kategorie „**nejvýznamnějších rizik**“ (ohodnocení vyšší než 30) spadá více jak 87 % výše zmiňovaných rizik. Zbylých 13 % rizik spadá do kategorie „**středně významných rizik**“

(s ohodnocením od 10 do 30). U celkového ohodnocení rizik byla zjištěna hodnota 256, což pokud se vypočte průměrná hodnota (32), spadá celkové hodnocení rizik do kategorie „**nejvýznamnějších rizik**.“

4.2 Metoda „PNH“

Metoda „PNH“ je jednoduchou polo-kvantitativní analytickou metodou, pomocí které se vyhodnocuje příslušné riziko ve třech jeho složkách, a to s ohledem na:

- pravděpodobnost vzniku (**P**),
- pravděpodobnost následků (**N**)- závažnost,
- názor hodnotitelů (**H**).

P- PRAVDĚPODOBNOST VZNIKU A EXISTENCE NEBEZPEČÍ	
Nahodilá	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Trvalá	5

Tabulka 8- Pravděpodobnost vzniku a existence nebezpečí [Zdroj:13]

N- MOŽNÉ NÁSLEDKY OHROŽENÍ	
Poškození zdraví (bez prac. neschopnosti)	1
Absenční úraz (s prac. neschopností)	2
Vážnější úraz vyžadující hospitalizaci	3
Těžký úraz a úraz s trvalými následky	4
Smrtelný úraz	5

Tabulka 9- Možné následky ohrožení [Zdroj: 13]

H- NÁZOR HODNOTITELE	
Zanedbatelný vliv na míru nebezpečí a ohrožení	1
Malý vliv na míru nebezpečí a ohrožení	2
Větší, nezanedbatelný vliv na míru ohrožení a nebezpečí	3
Velký a významný vliv na míru ohrožení a nebezpečí	4
Více významných a nepříznivých vlivů na závažnost a následky ohrožení a nebezpečí	5

Tabulka 10- Názor hodnotitele [Zdroj: 13]

Rizikový stupeň	R	Míra rizika
I.	> 100	Nepřijatelné riziko
II.	$51 \div 100$	Nežádoucí riziko
III.	$11 \div 51$	Mírné riziko
IV.	$3 \div 10$	Akceptovatelné riziko
V.	< 3	Bezvýznamné riziko

Tabulka 11- Celkové hodnocení rizika [Zdroj: 13]

V tabulce (11) je bodovým rozpětím vyjádřena naléhavost úkolů, přijetí opatření ke snížení rizika a priorit bezpečnostních opatření, které by měly být obsaženy v plánu pro zvýšení úrovně bezpečnosti, jenž by měl být součástí dokumentace rizik.

Při stanovení stupně závažnosti vyhodnocených rizik je možné rozdělení rizika do pěti stupňů (I. až V.):

- **I. Nepřijatelné riziko s katastrofickými důsledky:** vyžaduje okamžité zastavení činnosti, odstavení provozu do doby realizace nezbytných opatření a nového vyhodnocení rizik;
- **II. Nežádoucí riziko:** zde je vyžadováno urychlené provedení odpovídajících bezpečnostních opatření, které sníží riziko na akceptovatelnou úroveň. Na snížení rizika je nutno přidělit potřebné zdroje;
- **III. Mírné riziko:** v tomto případě, i když není nutnost opatření tak závažná jako u II. kategorie, je nutno z pravidla realizovat bezpečnostní opatření dle zpracovaného plánu podle rozhodnutí vedení podniku. Prostředky určené na snížení rizika je nutno implementovat ve stanoveném časovém období;
- **IV. Akceptovatelné riziko:** jedná se o stupeň rizika, který je přijatelné se souhlasem vedení. Nutností je zvážení nákladů na případné řešení nebo zlepšení. V případě že se nepodaří provést specifická bezpečnostní opatření za účelem snížení rizika, je potřeba zavést vhodná opatření organizační- běžný dozor, školení obsluhy;
- **V. Bezvýznamné riziko:** u tohoto případu nejsou vyžadována žádná zvláštní bezpečnostní opatření. Nejedná se však 100% bezpečnost, a proto je nutné na možné existující riziko včas upozornit a uvést např. jaká organizační či výchovná opatření je třeba realizovat. [13]

4.3 Vyhodnocení rizik v podniku PEDST- metoda „PNH“

V tabulce (12) je pomocí jednoduché polo-kvantitativní analytické metody „PNH“ provedena analýza rizik ve firmě PEDST. Do analýzy jsou zakomponovány zpozorovaná rizika, která mohou mít při současné úrovni zabezpečení dopad na podnik a následné vzniknutí újmy či ztrát.

Druh činnosti	Zdroj rizika	Identifikace nebezpečí	Vyhodnocení závažnosti rizika				Opatření k omezení rizika
Možnost vniku do areálu a pohyb neoprávněných osob	Chybějící vrcholová zábrana	Ztráta majetku firmy	P 4	N 4	H 3	R 48	Instalace vrcholových zábran
	Chybějící závora	Narušení bezpečnosti					Instalace závory
	Chybějící kamerový systém, výstražné tabule	Poškození majetku firmy					Instalace kamerového systému, výstražných tabulí
	Nepřítomnost hlídacího psa	Zdravotní újma					Pořízení hlídacího psa
Založení požáru							

Tabulka 12- Polo-kvantitativní metoda „PNH“ [Zdroj: vlastní]

Po aplikaci „PNH“ analýzy bylo zjištěno, že míra rizika **R** spadá do kategorie „**Mírné riziko**“. – „Bezpečnostní opatření nutno zpravidla realizovat dle zpracovaného plánu podle rozhodnutí vedení podniku. Prostředky na snížení rizika musí být implementovány ve stanoveném časovém období. Je-li toto riziko spojeno se značnými nebezpečnými následky, musí se provést další zhodnocení, aby se přesněji stanovila pravděpodobnost vzniku úrazu, jako podklad pro stanovení potřeby dosažení zlepšení a snížení rizika.“ [13]

5 NÁVRH NA REDUKCI VYBRANÝCH BEZPEČNOSTNÍCH RIZIK V PODNIKU PEDST

V kapitole jsou vypsána vybraná bezpečnostní rizika nacházející se v podniku PEDST a návrhy na jejich redukcí popř. minimalizaci. Ne vždy je potřeba řešit každou bezpečnostní skulinu či malý nedostatek instalací velmi nákladných bezpečnostních prvků. Takovéto prvky by sice mohly mít a určitě i měly patřičný výsledek, ale jak je zmíněno v kapitole (1), je neefektivní vynakládat na opatření bezpečnostních prvků vyšší náklady, než je samotná hodnota chráněného aktiva. Z praxe jsou známy případy kdy, pokud se patřičnými způsoby zapůsobí na psychiku aktéra, může dojít ke stejnému odrazení nežádoucího pachatele od jeho úmyslu, jako při instalaci o hodně nákladnějších bezpečnostních opatření. V tomto případě se jedná např. o:

- výstražné tabule jako na obrázcích (9, 10),
- vrcholové zábrany obrázek (11),
- kamerový systém obrázek (12, 14).



Obrázek 9- Výstražná tabule I [Zdroj: 7]

Instalace výstražných tabulí v areálu podniku, může mít vliv na snížení počtu neoprávněných pokusů o vniknutí do podniku, ať už za účelem vandalizmu či vlastního obohacení nežádoucího pachatele. Výstražné tabule tohoto typu mají za úkol informovat přítomné osoby, že okolí, ve kterém se právě pohybují, je monitorováno bezpečnostními kamerami. Takový akt, ať už pravdivý či milný, pak může mnoho potenciálních pachatelů odradit od jejich úmyslu, a to obzvláště, pokud je pachatel neznalý okolí a rozmístění kamerového systému či si není jist, jestli se opravdu pod dozorem nachází.

Obdobněpsychologický efekt, jako výstražné tabule s upozorněním na přítomnost kamerového systému, mohou mít výstražné tabule s upozorněním na přítomnost hlídacího psa- obrázek (10).



Obrázek 10- Výstražná tabule II [Zdroj: 7]

Existuje mnoho typů a variant provedení bezpečnostních tabulí, v tabulce (13) jsou vypsané konkrétní pořizovací údaje k výstražným tabulím na obrázcích(9 a 10).

Typ výstražné tabule	Materiál	Rozměr tabule	Cena za jednotku bez DPH	Cena za 50 ks bez DPH
Objekt střežen kamerami se záznamem	Plast	A5 - 210 x 148,5 mm	9,- Kč	450,- Kč
Objekt střežen psy	Plast	A3 - 420 x 297 mm	33,- Kč	1650,- Kč

Tabulka 13- Pořizovací údaje bezpečnostních tabulí [Zdroj: 7]

Jak už bylo zmíněno v kapitole (4), areál podniku PEDST je obklopen OO bez vrcholových zábran. V případě instalace vrcholových zábran v podobě ostnatého nebo žiletkového drátu na dosavadní OO jako na obrázku (11), by došlo k navýšení bezpečnostního stupně u OO. Zároveň by takovéto kroky mohly vést k odrazení nežádoucího pachatele od úmyslu vniknout do areálu nebo k snížení či úplné eliminaci neoprávněných vniknutí do areálu a následné zvýšení bezpečnosti chráněných aktiv. Jako další opatření pro eliminaci rizik je možné požit jiné prvky OO. Takovým prvkem může být např. bezpečnostní oplocení jako na obrázku (11), kdy už samotná konstrukce ochrany je vytvořena tak, aby co nejvíce znesnadňovala její překonání. Takovéto prvky OO je možno použít např. v kombinaci s podkopovými zábranami.



Obrázek 11- Vrcholová zábrana [Zdroj:20]

V tabulce (14) jsou vypsané pořizovací údaje vrcholových zábran jako na obrázku (11), které je možno použít při instalaci vrcholových zábran. Z tabulky (14) je možno vyčíst, že pokud by se pro instalaci vrcholové zábrany použila žiletková páska místo žiletkového drátu, došlo by na 600 m materiálu k úspoře větší než 23 000,- Kč.

Typ vrcholové zábrany	Ø drátu / vč. poplastování (mm)	Povrchová úprava	Běžných metrů v balení	Cena za jedno balení vč. DPH	Cena za 600 m vč. DPH
Ostnatý drát	1,6-1,7	Zn	100 m	401,80,- Kč	2410,80,- Kč
	1,5-1,7/2,1-2,7	Zn + plastovaný		535,80,- Kč	3214,80,- Kč
Žiletkový drát-spirálový	Ø spirály 45 cm	Zn	8 až 10 m	468,20,- Kč	28 092,- Kč
Žiletková páska		Zn	50 m	394,20,- Kč	4730,40,- Kč

Tabulka 14- Pořizovací údaje vrcholových zábran [Zdroj: 20]

I přes to, že je areál podniku PEDST chráněn SBS, se může stát, že dojde k narušení bezpečnosti a vniku neoprávněného pachatele do areálu podniku. K takovému činu může dojít jak za denního světla, kdy je areál přístupný veřejnosti, tak během noční směny POs např. v dobu, kdy nebude provádět obchůzku po areálu. Díky současnému stavu zabezpečení podniku a celkové hodnotě majetku, který se v podniku nachází, by se dalo říct, že podnik svým stavem doslova „dává možnost“ pachatelům k páčání trestné činnosti. Patříčným krokem pro eliminaci tohoto rizika by mohla být instalace kamerového

systemu po celém areálu. Správné rozmístění a typ kamer v areálu, jako např. na obrázku (12), by mohlo vykompenzovat takové bezpečnostní nedostatky, jakými jsou:

- značné možnosti ukrytí pro potenciální narušitele,
- nepřítomnost psa,
- služba POs pouze od 18:00 do 06:00 hodin.



Obrázek 12- Bezpečnostní kamera [Zdroj:25]

Na obrázku (13) je zobrazen záznam z venkovních bezpečnostních kamer, pořízený v rozdílnou denní dobu, kde je možno vidět, použije-li se kvalitní bezpečnostní kamera, vysoká kvalitu snímaného obrazu i ve špatných světelných podmínkách.



Ve dne



Ve dne



V noci



V noci

Obrázek 13- Kamerový snímek den, noc [Zdroj:12]

Zapůsobení na psychiku a následné odrazení pachatele od jeho úmyslu je možné vyvolat i tzv. atrapy kamerového systému jako na obrázku (14). Jedná se o model kamerového systému, který je po vizuální stránce totožný jako nákladné, instalované kamerové systémy.

Atrapy bezpečnostních kamer patří mezi jedny z neúčinnějších bezpečnostních prvků, které slouží k zastrašení nežádoucího pachatele. Ze statistik vyplývá, že pokud dojde k instalaci takového bezpečnostního opatření, pravděpodobnost spáchání trestného činu může až několikanásobně klesnout. Předností takového modelu bezpečnostní kamery mimo jeho vysokou účinnost proti možným nežádoucím pachatelům je, že cena za jednotku se pohybuje v řádu několika stovek korun, kdežto u klasických kamerových přístrojů, které slouží pro monitoring okolí, se cena může pohybovat v řádech desítek tisíc korun. Nevýhodou modelu kamery je, že slouží pouze k odrazení pachatele a vyvolání dojmu monitoringu podniku, nikoliv však pro samotný monitoring či pořizování záznamu. Atrapy bezpečnostních kamer, lze však kombinovat s funkčním kamerovým systémem, díky kterému pak pachatel neví, jestli je snímán skutečnou bezpečnostní kamerou nebo jen její atrapou. Může pak dojít k tomu, že zatímco se bude pachatel ukrývat před atrapou, bude snímán jinou bezpečnostní kamerou ukrytou na místě, kde by ji nečekal.



Obrázek 14- Atrapa bezpečnostní kamery [Zdroj:25]

V tabulce (15) je vytvořený a popsán kamerový set, který je možno aktuálně použít např. k zabezpečení menšího objektu, apod. Po rozšíření, kdy je možno k záznamovému zařízení připojit až 16 kamer, je možno celý set využít např. k zabezpečení areálu podniku či větších výrobních hal, apod.

Kamerový set s PROFI kamerami	
	VR záznamové zařízení
	- ovládání v češtině
	- nahrávání při pohybu
	- sledování přes internet
	- přístup přes mobilní telefon
	- ovládání myší
možnost modelu pro 4, 8 nebo 16 kamer	
	1 000GB pevný disk pro ukládání záznamů
	- vydrží na 2-4 týdny záznamu podle pohybu
	- možnost až 2,0TB
	4x kamera
	- rozlišení kamery 700 TV řádků
	- infra přísvit do 25 metrů
	ANTIVANDAL provedení
	- venkovní kryt
	- zoom v rozsahu 30°-95°
- snímací čip Sony Effio	
	napájecí zdroj pro kamery
	kabeláž na míru
	- včetně konektorů
	- kabeláž pro napájení i video
	- kabeláž připravíme dle požadavků
Cena kompletu: 18 890,-Kč bez DPH	

Tabulka 15- Kamerový set [Zdroj:12]

Pro minimalizaci nebo úplnou eliminaci rizika souvisejícího s činností a provozem SBS je možno použít tzv. pult centralizované ochrany. Jedná se o významný prvek v oblasti zabezpečení jak majetku podniku, tak i soukromého majetku. Instalace takového bezpečnostního opatření nese několik výhod, jsou jimi převážně:

- vyloučení zranění POs pokud dojde k porušení bezpečnosti

- není nutné vynakládat výdaje na proškolení vlastních zaměstnanců či POs v oblasti bezpečnosti
- vyloučení selhání lidského faktoru ze strany POs
- není nutná přítomnost POs
- areál pod stálým dozorem
- minimalizace rizika souvisejícího s přehlédnutím či nepovšimnutím pachatele pracovníkem ostrahy

ZÁVĚR

V bakalářské práci jsem se zaměřil na řešení problému analýzy ochrany, kterou je zabezpečení majetek v podniku PEDST.

V teoretické části jsem se věnoval literární rešerši, ve které jsem stručně definoval skladbu majetku podniku, možné způsoby pro zajištění jeho bezpečnosti a vymezil pojem bezpečnostní analýza podniku a metody k provádění této analýzy. Dále jsem v teoretické části vypracoval grafické vyjádření nejčastějších metod, které jsou použity pachateli pro vloupávání do objektů, nejčastější místa vniknutí do objektů a tabulkově znázornil kriminalitu v jihomoravské kraji a jeho okresech za rok 2013.

V praktické části jsem se zabýval posouzením současného stavu zabezpečení podniku PEDST z hlediska zajištění bezpečnosti, analýzou vybraných bezpečnostních rizik a návrhem na jejich redukci. Pomocí metod analýzy a sběru dat jsem se zaměřil na posouzení aktuálního bezpečnostního stavu obvodové ochrany a jednotlivých budov v podniku PEDST. Dále jsem se zaměřil na výčet nedostatků a zranitelných míst, které se v podniku PEDST nachází a na jejich redukci. Pomocí analytických metod jako jsou metoda „PNH“ a metoda Semikvantitativního hodnocení rizika jsem vypracoval analýzu na možná hrozící rizika v podniku. Za největší bezpečnostní nedostatky nacházející se v podniku PEDST považuji špatnou úroveň obvodové ochrany, absenci kamerového systému a množství nestřežených míst. V závěru praktické části jsem se zabýval návrhem na redukci zpozorovaných rizik a uvedl možné prostředky pro jejich minimalizaci.

V závěru práce doporučuji instalaci kamerového systému a modernizaci obvodové ochrany včetně instalace vrcholových zábran.

SEZNAM POUŽITÉ LITERATURY

- [1] Bezpečnostní analýza. In: *Risk analysis consultants* [online]. 2010 [cit. 2014-03-19]. Dostupné z: [http://www.rac.cz/rac/homepage.nsf/CZ/SS/\\$FILE/RAC%20Bezpecnostni%20analyza_Datasheet_CZ_100517%20Screen.pdf](http://www.rac.cz/rac/homepage.nsf/CZ/SS/$FILE/RAC%20Bezpecnostni%20analyza_Datasheet_CZ_100517%20Screen.pdf)
- [2] Česká republika. Kamerové systémy: Související legislativa: o obecní policii. In: <http://www.mvcr.cz/clanek/kamerove-systemy.aspx?q=Y2hudW09Mw%3d%3d>. 1991.
- [3] Česká republika. Kamerové systémy: Související legislativa: o obcích. In: <http://www.mvcr.cz/clanek/kamerove-systemy.aspx?q=Y2hudW09Mw%3d%3d>. 2000.
- [4] Česká republika. Kamerové systémy: Související legislativa: o ochraně osobních dat, ve znění pozdějších předpisů. In: <http://www.mvcr.cz/clanek/kamerove-systemy.aspx?q=Y2hudW09Mw%3d%3d>. 2000.
- [5] Česká republika. Kamerové systémy: Související legislativa: o Policii České republiky. In: <http://www.mvcr.cz/clanek/kamerove-systemy.aspx?q=Y2hudW09Mw%3d%3d>. 2008.
- [6] Česká republika. O ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. In: <http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/uplne-zneni-zakona-c-4122005/>. 2005.
- [7] E-tabulky. *Bezpečnostní tabulky* [online]. [cit. 2014-04-22]. Dostupné z: <http://www.e-tabulky.cz/bezpecnostnitabulky>
- [8] Elektronické zabezpečovací systémy (EVS). *Flexcom.s.r.o* [online]. [cit. 2014-03-19]. Dostupné z: <http://elektro.flexcom.cz/index.php/Elektronicke-zabezpecovaci-systemy-EVS.html>
- [9] Famikl: Bezpečnostní vložky. [online]. [cit. 2014-04-23]. Dostupné z: <http://www.famikl.cz/cenik/vlozky-do-dveri/>
- [10] HNILICA, Jiří a Jiří FOTR. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování*. 1. vyd. Praha: Grada, 2009, 262 s. ISBN 978-80-247-2560-4.
- [11] HRUŠKA, Miroslav. *Majetek podniku*. 2008. Dostupné z: http://www.obakakarvina.cz/09_vystupy.html
- [12] Kamerové a zabezpečovací systémy. *Kamerové systémy Ostrava* [online]. [cit. 2014-04-22]. Dostupné z: <http://www.kamerovesystemyostrava.cz/cctv/kamery-analogove.php>
- [13] KOUDELKA, Ctirad a Václav VRÁNA. *Rizika a jejich analýza*. VŠB – TU Ostrava Fakulta elektrotechniky a informatiky, 2006. Dostupné z: <http://fe1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf>
- [14] Kriminálnita v Jihomoravském kraji: Trestné činy zjištěné a objasněné na 1 000 obyvatel v okresech Jihomoravského kraje v letech 2007 až 2011. In: *Český statistický úřad* [online]. 2013 [cit. 2014-03-19]. Dostupné z: http://www.czso.cz/xb/redakce.nsf/i/kriminalita_v_jihomoravskem_kraji

- [15] Kriminalita v Jihomoravském kraji a jeho okresech v 1. až 2. čtvrtletí 2013. In: *Sčítání lidu, domů a bytů* [online]. 2013 [cit. 2014-03-19]. Dostupné z: [http://www.scitani.cz/csu/2013edicniplan.nsf/t/CD00217E79/\\$File/64130213q2p1.pdf](http://www.scitani.cz/csu/2013edicniplan.nsf/t/CD00217E79/$File/64130213q2p1.pdf)
- [16] LUDĚK, Lukáš a kolektiv. *Bezpečnostní technologie, systémy a management I*. 1. vyd. Zlín: VeRBuM. ISBN 978-808-7500-057.
- [17] LUDĚK, Lukáš a kolektiv. *Bezpečnostní technologie, systémy a management II*. Zlín: VeRBuM, 2012. ISBN 978-808-7500-194.
- [18] MARCELA, Vedralová. SOŠ INFORMATIKY A SPOJŮ A SOU, Kolín. *Ekonomika: Majetek podniku*. Prezentace. Kolín, 2009. Dostupné z: <http://www.soskolín.cz/studium/eko2.ppt>
- [19] *Perspektivní bezpečnostní technologie ochrany majetku: mezinárodní bezpečnostní konference: PYROS/ISSET 2008 : Brno, 15. května 2008*. Ve Zlíně: Univerzita Tomáše Bati, 2008?, 1 CD-R. ISBN 978-80-7318-699-9.
- [20] Ploty na klíč. In: *Moravskoslezské drátovny* [online]. [cit. 2014-04-22]. Dostupné z: <http://www.ploty-na-klic.cz/pletivo/ziletkovy-drat>
- [21] Projektové řízení: Řízení rizik projektu. In: *VBC Czech s.r.o.* [online]. [cit. 2014-03-19]. Dostupné z: <http://www.vbcczech.cz/rizeni-rizik-projektu.htm>
- [22] Provozování kamerového systému z hlediska zákona o ochraně osobních údajů. In: *Úřad pro ochranu osobních údajů* [online]. Praha, 2006 [cit. 2014-03-19]. Dostupné z: www.uoou.cz/files/stanovisko_2006_1.pdf
- [23] ŠEFČÍK, Vladimír. *Analýza rizik*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 98 s. ISBN 978-80-7318-696-8.
- [24] Technologie: Elektronická zabezpečovací signalizace. In: *Alkomsecurity a.s.* [online]. [cit. 2014-03-19]. Dostupné z: <http://www.alkom.cz/sluzby/technologie/elektronicka-zabezpecovaci-signalizace-ezs/>
- [25] Tegus. *Bezpečnostní kamerové systémy* [online]. [cit. 2014-04-22]. Dostupné z: <http://www.tegus.cz/kamerove-systemy/c-1188/>
- [26] UHLÁŘ, Jan. *Technická ochrana objektů*. Vyd. 1. Vydavatelství PA ČR, 2006, 246 s. ISBN 80-725-1235-8.
- [27] UNMZ. *ČSN seznam* [online]. [cit. 2014-03-29]. Dostupné z: <http://www.seznamcsn.unmz.cz/>
- [28] VALOUCH, Jan. *Projektování integrovaných systémů*. Prezentace. Ústav bezpečnostního inženýrství Fakulta aplikované informatiky, UTB ve Zlíně, 2011.

SEZNAM OBRÁZKŮ

<i>Obrázek 1- Druhy majetku v podniku [Zdroj: 18].....</i>	<i>9</i>
<i>Obrázek 2- Znárodnění oběžného majetku v podniku [Zdroj: 18].....</i>	<i>11</i>
<i>Obrázek 3- Vzájemné vztahy mezi hrozbou, protiopatřením, aktivem</i>	<i>16</i>
<i>Obrázek 4- Areál podniku [Zdroj: vlastní].....</i>	<i>26</i>
<i>Obrázek 5- Situační plán podniku [Zdroj: vlastní]</i>	<i>30</i>
<i>Obrázek 6- Obvodová ochrana I [Zdroj: vlastní].....</i>	<i>35</i>
<i>Obrázek 7- Obvodová ochrana II [Zdroj: vlastní]</i>	<i>35</i>
<i>Obrázek 8- Obvodová ochrana III [Zdroj: vlastní]</i>	<i>36</i>
<i>Obrázek 9- Výstražná tabule I [Zdroj: 7].....</i>	<i>41</i>
<i>Obrázek 10- Výstražná tabule II [Zdroj: 7]</i>	<i>42</i>
<i>Obrázek 11- Vrcholová zábrana [Zdroj: 20]</i>	<i>43</i>
<i>Obrázek 12- Bezpečnostní kamera [Zdroj: 25]</i>	<i>44</i>
<i>Obrázek 13- Kamerový snímek den, noc [Zdroj:12].....</i>	<i>44</i>
<i>Obrázek 14- Atrapa bezpečnostní kamery [Zdroj: 25]</i>	<i>45</i>

SEZNAM TABULEK

<i>Tabulka 1- Rozdělení metod bezpečnostní analýzy [Zdroj: 28]</i>	14
<i>Tabulka 2- Řešení bezpečnostních rizik v organizaci [Zdroj: 28].....</i>	15
<i>Tabulka 3- Stupnice měření poklesu zisku a vzrůstu investičních nákladů [Zdroj: 10].....</i>	17
<i>Tabulka 4- Kriminálnita v Jihomoravském kraji a jeho okresech v roce 2013 [Zdroj: 15]</i>	20
<i>Tabulka 5- Přehled českých technických norem [Zdroj: 27]</i>	22
<i>Tabulka 6- Prvky pro zabezpečení vchodových dveří [Zdroj:9]</i>	31
<i>Tabulka 7- Semikvantitativní hodnocení rizika [Zdroj: vlastní].....</i>	37
<i>Tabulka 8- Pravděpodobnost vzniku a existence nebezpečí [Zdroj: 13]</i>	38
<i>Tabulka 9- Možné následky ohrožení [Zdroj: 13]</i>	38
<i>Tabulka 10- Názor hodnotitele [Zdroj: 13].....</i>	38
<i>Tabulka 11- Celkové hodnocení rizika [Zdroj: 13]</i>	39
<i>Tabulka 12- Polo-quantitativní metoda „PNH“ [Zdroj: vlastní]</i>	40
<i>Tabulka 13- Pořizovací údaje bezpečnostních tabulí [Zdroj: 7].....</i>	42
<i>Tabulka 14- Pořizovací údaje vrcholových zábran [Zdroj: 20].....</i>	43
<i>Tabulka 15- Kamerový set [Zdroj: 12]</i>	46
<i>Graf 1- Použití nejčastějších vniků pachatelů do objektu [Zdroj: 28]</i>	19
<i>Graf 2- Použití nejčastějších metod vloupání pachatelů [Zdroj: 28]</i>	19
<i>Graf 3- Trestné činy zjištěné a objasněné na 1 000 obyvatel v okresech Jihomoravského kraje v letech 2007 až 2011 (roční průměry) [Zdroj: 14]</i>	21

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BA	Bezpečnostní analýza
BOZB a PO	Bezpečnost a ochrana zdraví při práci a požární ochrana
CCTV	Centrální kamerový sledovací systém
ČSN	Česká technická norma
OO	Obvodová ochrana
pFO	Podnikající fyzická osoba
PO	Právnícká osoba
PNH	Analytická metoda
	P- pravděpodobnost vzniku
	N- pravděpodobnost následků
	H- názor hodnotitelů
POs	Pracovník ostražky
SBS	Soukromá bezpečnostní služba