


Bezpečnostní audit v distribuční firmě

A Security Audit in a Distribution Company

Bc. Bohdana Hanáková

Diplomová práce
2018

 Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Bohdana Hanáková**
Osobní číslo: **A16269**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **kombinovaná**

Téma práce: **Bezpečnostní audit v distribuční firmě**
Téma anglicky: **A Security Audit in a Distribution Company**

Zásady pro vypracování:

1. Seznamte se s problematikou bezpečnostních auditů.
2. Uveďte nezbytnou terminologii.
3. Popište bezpečnostní audit v obecné rovině.
4. Charakterizujte distribuční firmy s uvedením jejich specifik.
5. Rozeberte vstupní informace prováděného bezpečnostního auditu.
6. Stanovte zaměření a cíle bezpečnostního auditu.
7. Popište jednotlivé kroky plnění a zjištěné závěry.
8. Navrhněte konkrétní bezpečnostní opatření.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. LUKÁŠ, Luděk a kolektiv. **Bezpečnosti technologie, systémy a management II.** Vyd. 1. Zlín: Radim Bačuvčík – VeRBum, 2012, 387 s. ISBN 978-80-87500-19-4.
2. LUKÁŠ, Luděk a kolektiv. **Bezpečnosti technologie, systémy a management V.** Vyd. 1. Zlín: Radim Bačuvčík – VeRBum, 2015, 368 s. ISBN 978-80-87500-67-5.
3. BRABEC, František. **Ochrana bezpečnosti podniku.** Vyd. 1. Praha: EUROUNION, s.r.o., 1996, 203 s. ISBN 80-85858-29-0.
4. KAMENÍK, Jiří a kol. **Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur.** Vyd. 1. Praha: Aspi, a.s., 2007, 340 s. ISBN 978-80-7357-309-6.
5. BRABEC, František a kolektiv. **Hlídací služby.** Vyd. 1. Praha: EUROUNION, s.r.o., 1995, 259 s. ISBN 80-85858-12-6.
6. BRABEC, František a kolektiv. **Bezpečnost pro firmu, úřad, občana.** Vyd. 1. Praha: Nakladatelství Public History, 2001, 400 s. ISBN 80-86445-04-06.
7. SMEJKAL, Vladimír a Karel RAIS. **Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd.** Praha: Grada, 2013, 483 s. Expert (Grada). ISBN 978-80-247-4644-9.
8. ŠEFČÍK, Vladimír. **Analýza rizik.** Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 98 s. ISBN 978-807-3186-968.

Vedoucí diplomové práce:

Ing. Dora Lapková

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

8. prosince 2017

Termín odevzdání diplomové práce:

28. května 2018

Ve Zlíně dne 8. prosince 2017



doc. Mgr. Milan Adámek, Ph.D.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
vedoucí ústavu

Jméno, příjmení: Bc. Bohdana Hanáková

Název diplomové práce: Bezpečnostní audit v distribuční firmě


Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 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 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 práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové 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 práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové 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, dne 15. 5. 2018


.....
podpis diplomanta

ABSTRAKT

Cílem diplomové práce je udělat bezpečnostní audit pro konkrétní distribuční firmu. Teoretická část obsahuje základní terminologii, obecný popis bezpečnostního auditu a charakteristiku distribuční firmy. V praktické části jsou rozebrány vstupní informace bezpečnostního auditu, jeho zaměření a cíle, jednotlivé kroky plnění a zjištěné závěry. Na základě výsledků jsou navržena konkrétní bezpečnostní opatření.

Klíčová slova: bezpečnost, bezpečnostní audit, bezpečnostní politika, hrozba, riziko, analýza rizik, řízení rizik

ABSTRACT

The aim of the diploma thesis is to make the security audit for the particular distribution company. The theoretical part includes basic terminology, a general description of the security audit and the characteristics of the distribution company. The security audit input, its focus and objectives, the individual steps of implementation and the findings are analyzed in the practical part. Specific security measures will be proposed on the basis of the results.

Keywords: safety, security audit, security policy, threat, risk, risk analysis, risk management

Ráda bych tímto poděkovala vedoucí mé diplomové práce paní Ing. Doře Lapkové, Ph.D za odborné vedení, cenné rady a připomínky při tvorbě práce. Dále velké poděkování patří i mé rodině, která mě po celou dobu ve studiu podporovala a byla mi oporou.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD	10
I TEORETICKÁ ČÁST	12
1 ZÁKLADNÍ TERMILOGIE	13
1.1 BEZPEČNOST	13
1.2 BEZPEČNOSTNÍ POLITIKA FIRMY	13
1.3 AKTIVUM	13
1.4 HROZBA	14
1.5 RIZIKO.....	15
1.6 ZRANITELNOST.....	15
1.7 ANALÝZA RIZIK.....	15
1.7.1 Stanovení hranice analýzy rizik	15
1.7.2 Identifikace aktiv	16
1.7.3 Stanovení hodnoty a seskupování aktiv	16
1.7.4 Identifikace hrozeb.....	16
1.7.5 Analýza hrozeb a zranitelností	16
1.7.6 Pravděpodobnost jevu	16
1.7.7 Měření rizika	16
1.7.8 Metody analýzy rizik.....	17
1.7.9 Metoda Kontrolní seznam	17
1.7.10 Metoda PNH.....	18
1.8 ŘÍZENÍ RIZIK.....	18
1.9 SHRNTÍ KAPITOLY	19
2 BEZPEČNOSTNÍ AUDIT V OBECNÉ ROVINĚ	20
2.1 CÍLE AUDITU	20
2.2 DRUHY AUDITU	21
2.2.1 Dělení z hlediska provedení	21
2.2.1.1 Interní audit.....	21
2.2.1.2 Externí audit.....	21
2.2.2 Dělení z hlediska komplexnosti	21
2.2.2.1 Komplexní bezpečnostní audit.....	21
2.2.2.2 Dílčí bezpečnostní audit.....	22
2.2.3 Dělení z časového hlediska	22
Pokud se na dělení BA podíváme z časového hlediska, můžeme ho rozdělit následovně:.....	22
2.2.3.1 Plánovaný audit.....	22
2.2.3.2 Mimořádný audit.....	22
2.2.3.3 Následný audit	22
2.3 OBLASTI BEZPEČNOSTNÍHO AUDITU	23
2.3.1 Objektová bezpečnost	23
2.3.1.1 Fyzická ostraha	25
2.3.1.2 Technická ochrana	26
2.3.2 Režimová opatření	27
2.3.3 Personální bezpečnost	28
2.3.4 Bezpečnost a ochrana zdraví při práci.....	28

2.3.5	Požární bezpečnost.....	29
2.3.6	Informační bezpečnost	31
2.4	PRŮBĚH AUDITU	33
2.4.1	Plánování.....	34
2.4.2	Příprava	34
2.4.3	Techniky auditorské práce	35
2.4.4	Realizační fáze	35
2.4.5	Zpracování závěrečné zprávy.....	36
2.4.6	Vyhodnocení auditu a fáze následné kontroly	37
2.5	SHRNUTÍ KAPITOLY	37
3	CHARAKTERISTIKA DISTRIBUČNÍ FIRMY.....	38
3.1	VYMEZENÍ POJMŮ.....	38
3.2	CÍLE LOGISTIKY.....	38
3.3	DISTRIBUCE VÝROBKŮ	39
3.4	SHRNUTÍ KAPITOLY	40
II	PRAKTICKÁ ČÁST	41
4	SEZNÁMENÍ S AUDITOVANOU FIRMOU	42
4.1	ZÁKLADNÍ ÚDAJE O SPOLEČNOSTI	42
4.2	ORGANIZAČNÍ STRUKTURA	42
4.3	PERSONÁLNÍ OBSAZENÍ	43
4.4	PRODEJNÍ SORTIMENT SPOLEČNOSTI.....	43
4.5	SHRNUTÍ KAPITOLY	44
5	POPIS A CHARAKTERISTIKA AREÁLU	45
5.1	STRUČNÝ POPIS AREÁLU.....	45
5.2	OBVODOVÁ OCHRANA AREÁLU	46
5.3	KONTROLNÍ PROPUSTKOVÁ SLUŽBA	47
5.4	FYZICKÁ OSTRAHA	49
5.5	SHRNUTÍ KAPITOLY	50
6	POPIS A CHARAKTERISTIKA VYBRANÉHO OBJEKTU	51
6.1	CHARAKTERISTIKA OBJEKTU.....	51
6.2	PLÁŠŤOVÁ OCHRANA	52
6.3	KLÍČOVÝ REŽIM	53
6.4	POŽÁRNÍ OCHRANA	54
6.4.1	Technická zpráva požární ochrany a požární řád.....	54
	Pro sklad je vypracována technická zpráva požární ochrany a požární řád.....	54
6.4.2	Věcné prostředky požární ochrany.....	56
6.4.3	Požárně bezpečnostní zařízení	58
6.4.4	Školení zaměstnanců a prevence v PO.....	59
6.5	BEZPEČNOST A OCHRANA ZDRAVÍ PŘI PRÁCI	60
6.6	INFORMAČNÍ BEZPEČNOST.....	63
6.6.1	Firemní informační systém	63
6.6.2	IT oddělení	63
6.6.3	Pracovní stanice uživatelů.....	64

6.7	SHRnutí KAPITOLY	65
7	BEZPEČNOSTNÍ AUDIT	66
7.1	ZAMĚŘENÍ A CÍLE AUDITU	66
7.2	VSTUPNÍ INFORMACE	66
7.3	ANALÝZA SOUČASNÉHO STAVU.....	68
7.4	ANALÝZA RIZIK.....	69
7.4.1	Identifikace aktiv.....	69
7.4.2	Identifikace hrozeb pomocí metody „Kontrolní seznam“.....	69
7.4.3	Analýza rizik pomocí metody polo-kvantitativní metody „PNH“	71
7.5	VYHODNOCENÍ SILNÝCH MÍST A NEDOSTATKŮ V JEDNOTLIVÝCH OBLASTECH BEZPEČNOSTI.....	74
7.5.1	Obvodová ochrana areálu.....	74
7.5.2	Kontrolní propustková služba	75
7.5.3	Fyzická ostraha.....	75
7.5.4	Plášťová ochrana	75
7.5.5	Klíčový režim.....	75
7.5.6	Požární ochrana	76
7.5.7	BOZP.....	76
7.5.8	Informační bezpečnost	77
7.6	ZÁVĚRY AUDITU.....	77
7.7	SHRnutí KAPITOLY	83
	ZÁVĚR	84
	SEZNAM POUŽITÉ LITERATURY.....	86
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	89
	SEZNAM OBRÁZKŮ	90
	SEZNAM TABULEK.....	91
	SEZNAM PŘÍLOH.....	92

ÚVOD

Bezpečnost osob i bezpečné prostředí v organizacích je velmi aktuální téma. V dnešní době vzrůstající kriminality, kybernetických útoků a dalších potencionálních hrozeb pro organizace, není radno tyto bezpečnostní hrozby podceňovat. Není také dobré zužovat bezpečnostní problematiku organizace pouze na jeden jediný konkrétní problém a snažit se ho vyřešit odděleně od ostatních. Bezpečnost organizace naopak zasahuje do všech jejich činností a její problematika je v pravém smyslu interdisciplinární a její zajištění souvisí s celou řadou dalších oborů, jako jsou ekonomika, informatika, životní prostředí, psychologie, personalistiky a další.

Aniž by si to mnohé firmy uvědomovaly, každá má svou bezpečnostní politiku. Vztah k bezpečnostní politice je v určitém smyslu ukazatelem řídicích schopností managementu, odkryje totiž schopnost chápat a rozlišovat věci podstatné a důležité pro správný chod organizace od těch nepodstatných. V dnešní době je v řadě firem bezpečnostní politika součástí její celkové firemní strategie. V každé organizaci by měla být samozřejmostí analýza slabých stránek, jejich vyhodnocení a následnou minimalizací rizik snížení na takovou úroveň, která bude zajišťovat bezpečnost v zásadních oblastech. Odhalení slabých míst a jejich náprava může být v dnešním velmi silném konkurenčním prostředí pro firmu zásadní. Vhodným nástrojem může být bezpečnostní audit, který ve své závěrečné fázi implementuje ideální nastavení bezpečnostní politiky v organizaci.

Hlavním podnětem ke zpracování daného tématu diplomové práce byla vlastní iniciativa zjistit, v jakém stavu se nachází bezpečnost v konkrétní distribuční společnosti. Po dobu mého 16 - letého působení ve firmě, totiž žádný takový bezpečnostní audit neproběhl. Dalším podmětem bylo určitým způsobem navázat na bakalářskou práci, jejímž tématem byla „Analýza rizik v distribuci a jejich minimalizace“. V této práci byla pomocí zvolených metod analýzy rizik vyhodnocena rizika, která ohrožují distribuční procesy vybrané obchodní společnosti. Některá navržená opatření společnost zavedla a tím došlo nejen k výrazným provozním úsporám, ale i ke zlepšení pracovních podmínek, zvýšení kvality poskytovaného servisu zákazníkům a konkurenceschopnosti velkoobchodu na českém trhu.

Cílem diplomové práce je udělat bezpečnostní audit pro konkrétní distribuční firmu. Teoretická část v první kapitole obsahuje základní terminologii spojenou s oblastí bezpečnosti a řízení rizik. V další kapitole je obecně popsán bezpečnostní audit, jeho

jednotlivé oblasti a kroky. Ve třetí kapitole je obecně charakterizována distribuční firma i se svými specifiky.

V praktické části je ve čtvrté kapitole nejdříve stručně charakterizována konkrétní distribuční firma, ve které je bezpečnostní audit proveden. Dále je popsán areál, kde společnost sídlí. V šesté kapitole je charakterizována budova distribuční společnosti a je analyzován současný stav plášťové ochrany, klíčového režimu ve firmě, požární ochrany, BOZP a taky informační bezpečnosti.

V závěrečné kapitole je zpracován samotný bezpečnostní audit v distribuční společnosti. Nejdříve je stanoven cíl a záměr auditu, následně je provedena prohlídka a analýza současného stavu ve společnosti, analýza dokumentace a vnitropodnikových směrnic souvisejících s bezpečností. Na základě zjištěných výsledků je stanoven závěr auditu, jehož součástí je navržení konkrétních bezpečnostních opatření, která by měla sloužit k minimalizaci rizik.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ TERMILOGIE

Pro správné a úplné pochopení problematiky bezpečnostního auditu, je nejdříve nutné definovat základní terminologii. V následující kapitole jsou vysvětleny pojmy, které jsou používány v této práci. Nejdůležitějším termínu „bezpečnostní audit“ a jeho jednotlivým krokům je věnována samostatná kapitola.

1.1 Bezpečnost

„Bezpečnost je stav, kdy jsou na nejnižší možnou míru eliminovány hrozby pro objekt (zpravidla stát, organizaci) a jeho zájmy, přičemž tento objekt je efektivně vybaven k redukci resp. eliminaci stávajících i potencionálních hroze a je ochoten při tomto procesu spolupracovat.“ [1]

1.2 Bezpečnostní politika firmy

Bezpečnostní politika firmy vychází z platné legislativy, představ managementu firmy o požadovaném způsobu ochrany, ze stanovených specifických bezpečnostních požadavků na zajištění bezpečnostních zájmů firmy a v neposlední řadě z finančních možností organizace.

Bezpečnostní politika definuje:

- způsob a postupy řešení ochrany bezpečnosti firmy,
- časové a finanční podmínky řešení,
- zásady havarijního plánování a jak jsou řešeny případné bezpečnostní incidenty,
- jakým způsobem je zajištěna ochrana bezpečnosti organizace. [2]

1.3 Aktivum

„Aktivem rozumíme vše, co má pro danou organizaci nějakou hodnotu, která může být zmenšena působením hrozby.“ [3]

Aktiva se člení na hmotná (např. peníze, lidé, nemovitosti, cenné papíry) a nehmotná (např. knowhow, kvalita zaměstnanců, informace, autorská práva, pověst firmy). Aktivem může být samotná organizace, jelikož hrozba může ohrožovat její existenci. Aktivum je charakterizováno svou hodnotou a zranitelností. Zranitelnost vyjadřuje jeho citlivost na působení hrozby.[3]

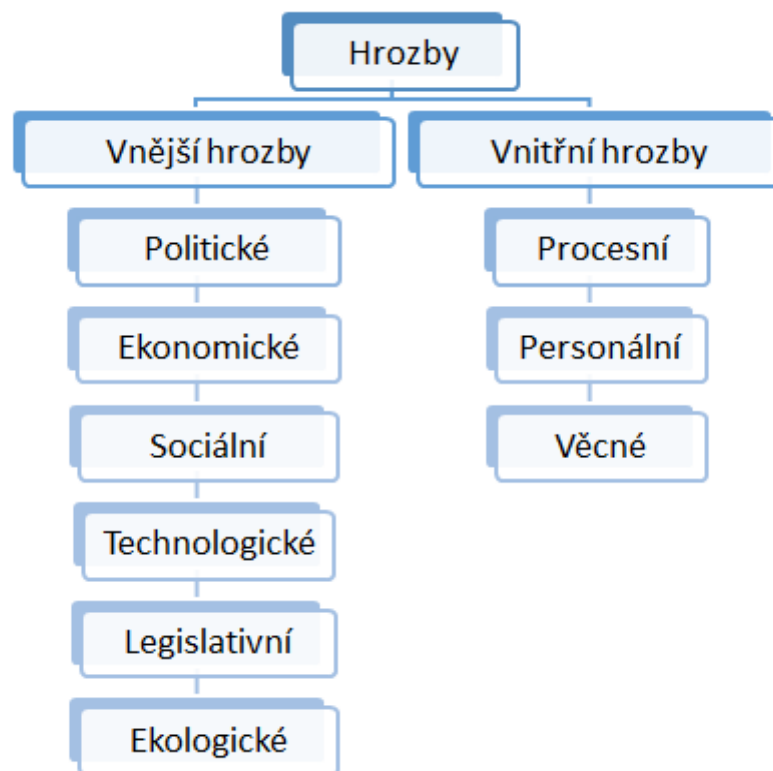
1.4 Hrozba

„Hrozba je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na aktiva nebo může způsobit škodu, resp. poškodit organizaci jako celek.“ [4]

Hrozba je charakterizována úrovní, která se hodnotí podle tří faktorů:

- nebezpečnost (schopnost hrozby způsobit škodu),
- přístup (pravděpodobnost, že se hrozba svým působením dostane k aktivu),
- motivace (zájem iniciovat hrozbu vůči aktivu). [3]

Hrozby mohou být lidského nebo přírodního původu, náhodné nebo úmyslné. Dále je možné hrozby klasifikovat z hlediska působení zdrojů hrozeb na firmu do dvou kategorií a to na vnější (neovlivnitelné) a vnitřní (ovlivnitelné) hrozby. Toto členění je znázorněno na obrázku č. 1.



Obr. 1. Členění hrozeb do kategorií [3]

1.5 Riziko

„Riziko vzniká vzájemným působením hrozby a aktiva a je vyjadřováno kombinací (resp. součinem) pravděpodobnosti výskytu mimořádné události a jejího dopadu na dané aktivum.“ [3]

„Riziko je tedy pravděpodobná újma způsobená dotčené osobě – nositeli rizika, vyjádřená buď penězi, nebo jinými jednotkami – počtem dnů pracovní neschopnosti, počtem lidských obětí.“[5]

Úroveň rizika je vyjádřena hodnotou aktiva. Na růstu této úrovně rizika se podílí nejenom úroveň hrozby a zranitelnosti, ale i hodnota aktiva. Riziko se sníží přijetím protiopatření. Při jeho návrhu je nutné dbát toho, aby vynaložené náklady na snížení rizika byly přiměřené hodnotě chráněných aktiv. Zbytkovým rizikem bývá označováno takové riziko, které je tak malé, že je pro organizaci přijatelné a není nutno přijímat další protiopatření k jeho snížení. Zbytkové riziko však může zůstat i po zavedení bezpečnostních opatření. [3]

1.6 Zranitelnost

„Zranitelnost představuje nedostatek, slabinu nebo stav analyzovaného aktiva, které může hrozba využít pro uplatnění svého nežádoucího vlivu.“[3]

Tato vlastnost aktiva vyjadřuje jeho citlivost na působení dané hrozby. Základní charakteristikou je úroveň zranitelnosti, která je stanovována dle citlivosti a kritičnosti. [3]

1.7 Analýza rizik

Analýza rizik (dále jen AR) je prvotním krokem v procesu snižování rizik, kdy jsou definovány rizika a jejich závažnost. Klade si za cíl poskytnout manažerům rizik podklady pro ovládání rizik a pro rozhodování o riziku.[5]

Samotná AR se skládá z níže uvedených kroků.

1.7.1 Stanovení hranice analýzy rizik

Hranicí analýzy rizik je nazývána pomyslná čára, která odděluje aktiva zahrnutá do analýzy od ostatních. Při jejím stanovování se vychází ze záměrů managementu organizace. Zahrnutá aktiva do AR leží uvnitř hranice a jsou to aktiva, ze kterých je subjekt složen. [4]

1.7.2 Identifikace aktiv

Při identifikaci aktiv se vytvoří seznam všech aktiv ležících uvnitř hranice AR. Uvede se jeho název, umístění a vlastník aktiva. [4]

1.7.3 Stanovení hodnoty a seskupování aktiv

Posuzuje se, jak velkou škodu přinese organizaci zničení nebo ztráta jednotlivých aktiv. Při stanovení hodnoty aktiva se většinou vychází z jeho nákladových charakteristik, v některých případech výnosových.

Jelikož obvykle bývá aktiv velké množství, snižuje se jejich počet tak, že se provede seskupení aktiv dle různých hledisek. Tak vzniknou skupiny aktiv s podobnými vlastnostmi a tato vytvořená skupina pak dále figuruje jako jedno aktivum.[4]

1.7.4 Identifikace hrozeb

Při identifikaci hrozeb se vybírají ty, které by mohly ohrožit alespoň jedno z aktiv organizace. [4]

1.7.5 Analýza hrozeb a zranitelností

V tomto kroku AR se hodnotí každá hrozba oproti každému aktivu. V případě těch aktiv, kdy se může na ně hrozba uplatnit, se stanovuje úroveň hrozby vůči tomuto aktivu a úroveň zranitelnosti aktiva proti této hrozbě. [4]

1.7.6 Pravděpodobnost jevu

Je to údaj, s jakou pravděpodobností tento jev může nastat. Vychází se z toho, že určitý soubor výchozích podmínek nemusí vždy vést k totožnému výsledku. Při počítání s pravděpodobnostmi se zkoumá, zda je jev náhodný či nikoliv, jestli patří do určitého intervalu. Při AR je nutné posoudit pravděpodobnost naplnění každého scénáře. [4]

1.7.7 Měření rizika

Výše rizika vyplývá z hodnoty aktiva, úrovně hrozby a zranitelnosti aktiva. Při AR se pracuje s veličinami, které nelze mnohdy přesně změřit, a určování jejich velikosti v mnoha případech spočívá pouze na kvalifikovaném odhadu odborníka na základě jeho zkušeností (zpravidla se používají výrazy typu „malý“, „střední“, „velký“, nebo stupnice 1-10). [4]

1.7.8 Metody analýzy rizik

K metodám AR lze přistupovat dvěma základními způsoby řešení, buď **kvantitativní**, nebo **kvalitativní** metodou. Často se oba tyto přístupy kombinují. Při výběru nejvhodnější metody a postupu analýzy je potřeba zvážit:

- dostupnost zdrojů – lidských, výpočetních a časových,
- cíl, kterého se má dosáhnout,
- zkušenosti osob s jednotlivými kroky a postupy analýzy rizik,
- velikost a složitost daného projektu,
- dostupnost informací. [4]

Kvantitativní metody jsou založeny na dvou základních krocích, na pravděpodobnosti výskytu jevu a pravděpodobnosti ztráty hodnoty. [5]

Kvalitativní metody vychází z matematických výpočtů rizika, z četnosti výskytu hrozby a jejího dopadu. Používá se číselné ocenění jak pro pravděpodobnost vzniku události, tak i pro oceňování dopadu dané události. Nejčastěji bývá riziko vyjádřeno pomocí roční předpokládané ztráty, které je uvedeno ve finanční částce, což je výhodou těchto metod. [4]

V praktické části diplomové práce byla pro zhodnocení rizik použita **metoda Kontrolní seznam** a **metoda PNH**.

1.7.9 Metoda Kontrolní seznam

Je to velmi jednoduchá technika, ve které se používá seznam položek, kroků či úkolů, podle kterých se ověřuje správnost či úplnost postupu. Analýza pomocí kontrolního seznamu často slouží jako základ pro různé sofistikované metody v oblasti kvality, bezpečnosti či rizik. Kontrolní otázky jsou obvykle generovány na základě seznamu charakteristik sledovaného systému nebo činností, které souvisí se systémem a případnými dopady, selháním článku systému a vznikem škod. Výsledek lze buď zaznamenat jen jako ano / ne – jak je vidět v tabulce č. 1, nebo lze kontrolnímu seznamu přiřadit více možností (např. téměř splňuje, je třeba ještě jedna kontrola atd.). Důležité je, aby kontrolní seznamy byly pravidelně prověřovány a aktualizovány. [5]

Tab. 1. Kontrolní seznam – pracovní list [14]

Kontrolní otázka / seznam	Odpověď ANO	Odpověď NE

1.7.10 Metoda PNH

Je to bodová polo-quantitativní metoda, pomocí které se vyhodnocuje příslušné riziko ve třech jeho složkách. Tyto složky jsou:

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

Pravděpodobnost vzniku rizika (P) je určena stupnicí 1–5, toto platí i pro stanovení pravděpodobnosti následků (N). Názor hodnotitelů (H) je rovněž hodnocen vzestupně číslem 1–5.

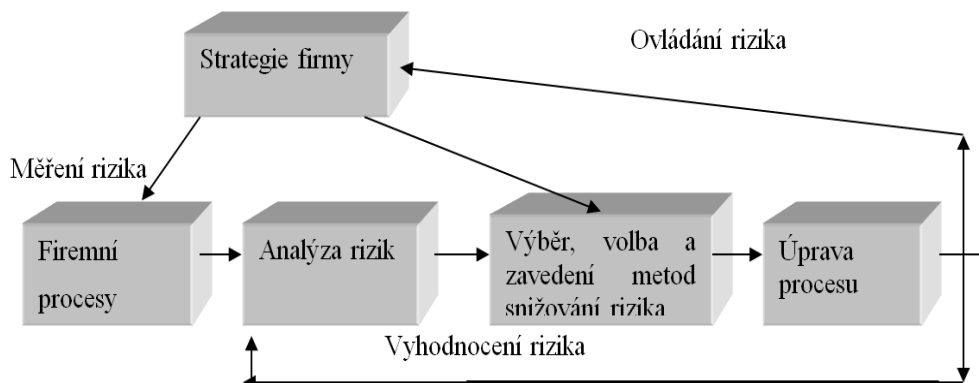
Součinem jednotlivých činitelů se určuje celkové hodnocení rizika, výsledkem je ukazatel míry rizika – **R**.

Výsledný rizikový stupeň určuje bodové rozpětí a vyjadřuje naléhavost přijetí vhodného opatření pro snížení rizika na přijatelnou úroveň. [4]

1.8 Řízení rizik

Činnost, která navazuje na AR, je proces řízení rizik. „Řízení rizik je vědecký přístup k řešení problému rizika, a to cestou jeho identifikace a měření, předvídání možných nahodilých ztrát a navrhování takových postupů a metod, které minimalizují výskyt a finanční dopad těch ztrát, které se ve firmě objeví.“ [4]

Tento proces je graficky znázorněn na obrázku č. 2.



Obr. 2. Proces řízení rizik ve firmě[4]

Náhody, neočekávané události, které se v minulosti nevyskytovaly vůbec nebo pouze minimálně, ještě více zvyšují riziko a jsou jedním z velkých problémů řízení rizik. Nejdůležitějším krokem je výpočet míry rizik a hodnocení rizik. Podle potencionálního peněžního či jiného existenčního dopadu ztráty se člení riziko do následujících skupin:

- **kritické riziko** – potencionální ztráty způsobí bankrot nebo krach firmy,
- **důležité riziko** – potencionální ztráty nevyústí v bankrot, ale svých významem přesahuje běžné hospodaření firmy,
- **běžné riziko** – potencionální ztráty mohou být pokryty stávajícími aktivy společnosti.

Čím vyšší je míra rizika, tím účinnější opatření musí být zavedena, aby se riziko eliminovalo nebo snížilo na přijatelnou úroveň. [4]

1.9 Shrnutí kapitoly

V první kapitole jsou definovány základní pojmy z oblasti bezpečnosti a řízení rizik, jako je bezpečnost, aktivum, hrozba, riziko, analýza rizik nebo řízení rizik. Dále jsou stručně popsány metody analýzy rizik a zvolené metody Kontrolní seznam a PNH pro praktickou část diplomové práce.

2 BEZPEČNOSTNÍ AUDIT V OBECNÉ ROVINĚ

Bezpečnostní audit (dále jen BA) je přezkoumání určitého konkrétního bezpečnostního opatření v konkrétním objektu nebo taky systematický proces objektivního ověřování, zajišťování a zhodnocení důkazů o bezpečnostní situaci. Cílem je objektivně porovnat skutečnost s požadovaným stavem bezpečnosti. Výsledkem BA je písemná zpráva pro vedení společnosti, zda je stav vyhovující či ne. V případě nevyhovujícího stavu je potřeba navrhnout nápravná opatření k odstranění neshod tak, aby byla zaručena ochrana organizace ve všech potřených oblastech. Bezpečnostní audit taky může ukázat managementu firmy, že finanční prostředky vynaložené na ochranu bezpečnosti jsou dostatečně a vhodně využity.

2.1 Cíle auditu

Smyslem a cílem auditu je za použití analytických, matematických, statistických aj. metod a technik následují:

- zjistit, zda existuje bezpečnostní politika podniku a zda jsou zpracovány bezpečnostní plány ochrany,
- zjistit, zda je zaveden systém jakosti, zda jeho jednotlivé prvky odpovídají požadavkům příslušných norem, směrnic, nařízení a jak jsou tyto požadavky uskutečněny,
- jaká jsou v objektu prováděna režimová opatření,
- jaká je v objektu nasazena bezpečnostní a protipožární technika,
- zda existují havarijní plány, ověřit jejich funkčnost a aktualizace,
- prověřit, jestli reálné procesy probíhají v souladu s dokumentovaným systémem stále a za všech okolností,
- ověřit, zda je implementace systému jakosti účinná, čili zda vytváří podmínky pro splnění požadavků zákazníka,
- přesně formulovat odhalené neshody, které jsou doloženy objektivními důkazy,
- navrhnout nápravná opatření s konkrétním termínem odstranění, jasnou a adresnou personální odpovědností výkonného pracovníka a odpovědného manažera. [7]

2.2 Druhy auditu

Bezpečností audit můžeme rozdělit z několika hledisek, např. podle toho, kdo BA ve firmě provede, z časového hlediska nebo z hlediska komplexnosti. [2]

2.2.1 Dělení z hlediska provedení

Z tohoto hlediska se BA dělí na interní a externí audit.

2.2.1.1 *Interní audit*

Interní audit provádí zaměstnanec firmy, většinou to bývá bezpečnostní manažer. Bezpečnostní manažer plánuje, organizuje, řídí a následně kontroluje bezpečnostní situaci ve firmě. U větších podniků je součástí bezpečnostního managementu, který je nezávislou jednotkou v organizaci a je odpovědný majitelům firmy.

Před zahájením BA si musí bezpečnostní manažer nejdříve prostudovat podklady z poslední prověrky dané části firmy. Je nutno podotknout, že pokud je nějaký konkrétní úsek ve firmě pod jeho vedením, tak zde nemůže vykonávat bezpečnostní audit a musí být jmenován jiný zkušený zaměstnanec z důvodu nezávislosti. [6]

2.2.1.2 *Externí audit*

V případě, že firma nemá vlastní bezpečnostního manažera nebo bezpečnostní problém je velmi specifický, obrací se organizace na externí specializovanou firmu, která se zabývá činností auditu bezpečnosti. Tyto firmy se opírají o profesionální tým zkušených auditorů, který při vstupní analýze dokáže nasměrovat nejen k typickým, ale i velmi specifickým problémům, které zaměstnanci firmy kvůli provozní „slepotě“ mnohdy nevidí. [6]

2.2.2 Dělení z hlediska komplexnosti

Z pohledu komplexnosti je BA dělen na komplexní a dílčí audit.

2.2.2.1 *Komplexní bezpečnostní audit*

U komplexního BA je předmětem auditu bezpečnost organizace jako celek. K tomuto náročnému kroku se přistupuje při definování bezpečnostní politiky podniku. Musí být zkontrolovány veškeré vnitřní i vnější skutečnosti, které ji ovlivňují. Je-li však komplex firemní bezpečnosti značně rozsáhlý a komplikovaný, hrozí pak, že budou opomenuty

vazby a vztahy k firmě jako celku a vzájemné vazby mezi jednotlivými organizačními složkami.

Pokud je již bezpečnostní politika v organizaci nastavena, je nutné provádět pravidelné kontroly, jestli nastavená opatření stále odpovídají realitě, jsou dostatečná a efektivní. [2]

2.2.2.2 Dílčí bezpečnostní audit

Tento audit řeší určitý výsek komplexu ochrany bezpečnosti a je zaměřen na konkrétní činnosti v organizaci. Přístupuje se k němu z důvodu větší přehlednosti, nebo pokud ostatní subsystémy komplexu bezpečnosti fungují bezproblémově a zádrhel se objevuje pouze v některém objektu nebo směru firemní bezpečnosti. [2]

2.2.3 Dělení z časového hlediska

Pokud se na dělení BA podíváme z časového hlediska, můžeme ho rozdělit následovně:

2.2.3.1 Plánovaný audit

Plánovaný audit se provádí v pravidelných a předem stanovených časových intervalech. S termíny jsou v předstihu seznámeni auditoři, aby měli dostatek času na prostudování potřebných podkladů. [6]

2.2.3.2 Mimořádný audit

Mimořádný bezpečnostní audit je prováděn při mimořádné události ve firmě, jako je např. změna majitelů firmy, změna bezpečnostní politiky, byl spáchán trestný čin v objektu organizace, došlo k pojistné události, zaměstnanec se dopustil protiprávního jednání atd. [6]

2.2.3.3 Následný audit

Pokud při plánovaném nebo mimořádném auditu byly zjištěny nesrovnalosti s bezpečnostní politikou organizace, je auditorem doporučen následný audit, jehož cílem je prověřit zavedení nápravných opatření. Termín se zapíše do závěrečné zprávy z auditu, která obsahuje doporučená nápravná opatření.[6]

2.3 Oblasti bezpečnostního auditu

Pokud chceme, aby byl BA proveden kvalitně, je potřeba vytyčený problém řešit a posuzovat ze všech hledisek, tedy komplexně.

V zásadě je nutné ve firmě ochraňovat následující tři skupiny aktiv:

- hmotný a nehmotný majetek,
- fyzické osoby,
- informace.

Pro dosažení požadovaného stupně zabezpečení se v praxi využívají tyto čtyři základní skupiny bezpečnostních opatření a prostředků:

- fyzická ostraha,
- technická ochrana,
- administrativně organizační a režimová opatření,
- kombinace předchozích prostředků a opatření. [8]

Na základě těchto skutečností dělíme audit do následujících oblastí.

2.3.1 Objektová bezpečnost

Při auditu objektové bezpečnosti kontrolujeme stav fyzického a technického zabezpečení objektu, zda vůbec existuje, či jeho efektivnost. Na obrázcích č. 3 a č. 4 jsou ukázky možných technických bezpečnostních prostředků. [7]



Obr. 3. Technický bezpečnostní prostředek – mechanický [7]



Obr. 4. Technický bezpečnostní prostředek – elektronický [7]

K ochraně vlastního nebo užívaného objektu vede podnik především vzrůstající majetková kriminalita, neustále narůstající objem škod a aktivní působení pojišťoven, které se tak kryjí před hrozbou náhrady vysokých škod.

Pokud se na vnější ochranu objektů podíváme z prostorového hlediska, tak ji můžeme rozdělit následovně na:

- **obvodovou** - obvod objektu je dán administrativní hranicí a u obvodové ochrany je důležité to, aby tato ochrana fungovala po celém obvodu objektu. Nejpoužívanější ochranou bývá různé oplocení, které by však bez doplňkové fyzické ostrahy nebo elektronického zabezpečovacího systému nemohlo bránit vniknutí do objektu. Obvodová ochrana zahrnuje jednak ochranu obvodu objektu a zajištění nepropustnosti a za další propustkové místa,
- **plášťovou** - jde o zajištění pláště objektu z hlediska možných rizik a většinou se k tomu využívá poplachový zabezpečovací a tísňový systém,
- **prostorovou** - u této ochrany je kladen důraz na celý prostor objektu, bez ohledu na různé oplocení. Je možné ji zajišťovat jak fyzickou ostrahou, tak technickými prostředky (např. snímání prostoru kamerami). [2]

2.3.1.1 Fyzická ostraha

Fyzická ostraha (dále jen FO) patří k nejstarší a stále k nejčastější formě zajišťování ochrany objektu a jako jediná v případě nutnosti je schopná zakročit k odvrácení nebezpečí. FO může být realizována jednak soukromými bezpečnostními službami, které mají tuto činnost jako předmět svého podnikání, jednak vlastními zaměstnanci.

Úkolem FO je zajistit ochranu majetku a osob, bezpečnost svěřených objektů a veřejný pořádek, čehož je dosahováno:

- kontrolní propustkovou službou,
- kontrolní činností,
- střežením objektů a prostor formou strážní služby,
- realizací bezpečnostních opatření v objektu,
- realizací zásahů při mimořádných událostech,
- vyrozuměním míst poskytujících pomoc,
- zajištěním dalších oprávněných zájmů zákazníka.

FO se dělí z různých hledisek následovně: z časového hlediska, podle rozsahu výkonu, podle způsobu zajištění, podle výzbroje a výstroje a podle vystupování na veřejnosti.

Z hlediska ochrany a ostraha objektů je možné formulovat následující formy FO:

- strážní služba,
- bezpečnostní dohled,
- bezpečnostní ochranný doprovod,
- bezpečnostní průzkum,
- kontrolní propustková služba,
- bezpečnostní výjezd – zásah. [2]

Na základě poznatků z dosavadní praxe soukromé bezpečnostní činnosti lze prozatím odvodit tyto metody FO:

- fyzického pozorování,
- osobní prohlídky a kontroly zavazadel,
- kontroly osob,
- kontroly vozidel a nákladů,
- kontroly stavu,

- kontroly dokladů,
- fyzických zábran a bariér,
- nasazení cvičeného psa,
- přesvědčování,
- obranných a ochranných zákroků,
- evakuačních a ochranných opatření,
- zajištění místa činu. [2]

2.3.1.2 Technická ochrana

„Technická ochrana představuje systémy a komponenty, pomocí nichž se vytvářejí relativně stálé podmínky bránící nepovolným osobám vniknout do chráněného objektu, ale rovněž systémy signalizující vznik požáru nebo signalizační systémy informující o změnách různých stavů, které mohou vést k haváriím apod.“ [2]

Technické prostředky dělíme podle základního technického principu, na němž jsou vyrobeny, následovně:

- mechanické zábranné systémy (dále jen MZS),
- poplachové zabezpečovací a tísňové systémy (dále jen PZTS).

MZS patří k nejstarším technickým zabezpečovacím prostředkům a mají zabránit neoprávněnému vniknutí do objektu. K MZS řadíme:

- mříže,
- zámky a bezpečnostní uzamykací systémy,
- závory,
- rolety,
- úschovné objekty,
- ploty,
- bezpečnostní dveře,
- bezpečnostní fólie a bezpečnostní skla. [2]

PZTS je technický systém, který slouží ke zjištění možné hrozby (vniknutí, pokus o vniknutí do střeženého objektu apod.) a předání včasné informace o situaci v chráněném prostoru. Obsluha těchto systémů vyvolá akci, která povede k vykonání zabezpečovacích úkonů. Pod informací se rozumí zvukový, obrazový, světelný signál apod. [9]

Dělí se následovně:

- poplachový zabezpečovací systém – slouží k detekování a signalizaci přítomnosti, vniknutí nebo pokusu o vniknutí vetřelce do střeženého prostoru,
- poplachový tísňový systém – poskytuje uživateli možnost úmyslného vyvolání poplachového stavu,
- poplachový zabezpečovací a tísňový systém – kombinovaný systém určený k detekci poplachu vniknutí a tísňového poplachu. [9]

Mezi PZTS patří:

- poplachová zabezpečovací signalizace,
- elektrická požární signalizace,
- kamerové systémy,
- vstupní systémy,
- komunikační systémy,
- dohledové a přijímací poplachové centrum,
- systém kontroly strážní služby,
- prostředky pro detekci látek,
- technické prostředky proti aktivnímu a pasivnímu odposlechu,
- tísňová tlačítka pro přivolání pomoci při zdravotních potížích a nouzi. [2]

2.3.2 Režimová opatření

Režimová opatření posuzují soulad platné legislativy s potřebami organizace, jakým způsobem spolupracují jednotlivé úseky, komunikaci a její dostatečnost mezi zaměstnanci a v neposlední řadě systém, úplnost a provázanost vnitropodnikových předpisů.

Režimová opatření platí pro:

- vnitropodnikové činnosti zaměstnanců,
- pohyb materiálu v rámci podniku,
- pohyb a chování osob, které přicházejí zvenku, včetně oběhu dokladů a informací uvnitř podniku,
- jakým způsobem budou prezentovány informace, data a dokumenty navenek. [8]

Všechny nutné pravidla by měly být zpracovány v patřičných organizačních normách. Další významnou činností, která se týká režimové ochrany, je spisová služba. Spisová služba je soubor činností a technických a věcných prostředků vedoucích ke správě dokumentů. Zajišťuje odbornou správu elektronických, listinných, i předmětových dokumentů. Jedná se o správu dokumentů doručených i vlastních, tato správa dokumentů probíhá po dobu celého životního cyklu dokumentu. [8]

2.3.3 Personální bezpečnost

Personální bezpečnost představuje nejméně spolehlivý faktor bezpečnostního prostředí z toho důvodu, že člověk je silně subjektivně ovlivnitelný, a tedy nestabilní element. Personální bezpečnost můžeme rozdělit na dvě oblasti – oblast personálního výběru vhodných osob a oblast personální práce s těmito lidmi. [6]

Personální výběr spočívá ve výběru vhodného budoucího zaměstnance na základě požadavků na konkrétní pozici. Rozhodující vliv na přijetí má úroveň profesních znalostí, vzdělání a celková schopnost vykonávat požadovanou práci.

Oblast personální práce zahrnuje především vstupní školení, následné další prohlubování profesních znalostí a taktéž průběžné hodnocení a kontrolu zaměstnanců. [6]

2.3.4 Bezpečnost a ochrana zdraví při práci

Zajištění bezpečnosti a ochrany zdraví při práci (dále jen BOZP) je základní povinností zaměstnavatele vůči zaměstnancům, která je stanovena především zákonem č. 262/2006 Sb., zákoníkem práce. Zaměstnavatel má dále zákonem stanoveno pravidelně seznamovat zaměstnance s právními a ostatními předpisy k zajišťování bezpečnosti práce, bezpečnosti technických zařízení a ochrany zdraví při práci. Je nutné pravidelně tyto znalosti předpisů ověřovat, vyžadovat a kontrolovat jejich dodržování. K tomuto účelu zaměstnávají organizace bezpečnostní pracovníky. [11]

Zákoník práce stanoví i povinnosti zaměstnanců, mezi které patří:

- dodržování právních předpisů k zajištění bezpečnosti práce, bezpečnosti technických zařízení a ochrany zdraví při práci, dodržování i zbylých předpisů,
- dodržování zásad bezpečnostního chování na pracovišti, stanovených pracovních postupů, se kterými byl pracovník řádně obeznámen,

- používat při práci osobní ochranné prostředky a ochranná zařízení. Slouží jako ochrana před úrazy, jsou to např. ochranná přilba – viz obrázek č. 5, ochranné brýle, chrániče uší, ochranné rukavice a oděv, bezpečnostní obuv nebo taky prostředky na ochranu dýchacích orgánů,



Obr. 5. Ochranný prostředek při práci – přilba [7]

- nepožívat v pracovní době alkoholické nápoje a jiné návykové látky na pracovištích, i mimo toto pracoviště, nenastupovat pod jejich vlivem do zaměstnání,
- dodržovat nařízený zákaz kouření,
- nahlašovat svému nadřízenému závady, které by mohly ohrozit bezpečnost zdraví při práci, a dle svých možností se podílet na jejich likvidaci atd. [11]

2.3.5 Požární bezpečnost

Požární bezpečností se dle vyhlášky č. 246/2001 Sb. (vyhláška o požární prevenci) rozumí: „Souhrn organizačních, územně technických, stavebních a technických opatření k zabránění vzniku požáru nebo výbuchu s následným požárem, k ochraně osob, zvířat a majetku v případě vzniku požáru a k zamezení jeho šíření.“ [14]

Tato vyhláška dále stanoví, jakým množstvím a druhy věcných prostředků požární ochrany a požárně bezpečnostními zařízeními mají být vybaveny prostory organizací. Toto vyplývá z požárně bezpečnostního řešení stavby, nebo z obdobné dokumentace, která je součástí projektové dokumentace. [14]

Do věcných prostředků požární ochrany řadíme:

- hasicí přístroje,
- osobní ochranné prostředky,
- prostředky pro záchranu a evakuaci osob (např. seskokové matrace, plachty a záchranné tunely, žebříky, hydraulické vyprošťovací zařízení, pneumatické vaky),
- prostředky pro práci ve výškách,
- prostředky pro práci s nebezpečnými látkami a pro dekontaminaci, analyzátoři plynů, kapalin a nebezpečných látek,
- požární výzbroj,
- spojovací a komunikační prostředky a technologie operačních středisek,
- hasiva a příměsi do hasiv,
- přenosné zásahové prostředky. [14]

Mezi požárně bezpečnostní zařízení patří:

- zařízení pro požární signalizaci (např. elektrická požární signalizace, zařízení pro detekci hořlavých plynů a par, ruční požárně poplachové zařízení),
- zařízení pro usměrňování pohybu kouře při požáru (např. zařízení pro odvod kouře a tepla, zařízení přetlakové ventilace, kouřová klapka včetně ovládacího mechanismu, kouřotěsné dveře, zařízení přirozeného odvětrání kouře),
- zařízení pro únik osob při požáru (např. požární nebo evakuační výtah, nouzové osvětlení, nouzové sdělovací zařízení, funkční vybavení dveří, bezpečnostní a výstražné zařízení),
- zařízení pro zásobování požární vodou (např. vnější požární vodovod včetně nadzemních a podzemních hydrantů, plnicích míst a požárních výtokových stojanů,

vnitřní požární vodovod včetně nástěnných hydrantů, hadicových a hydrantových systémů, nezavodněné požární potrubí),

- zařízení pro omezení šíření požáru (např. požární klapka, požární dveře a požární uzávěry otvorů včetně jejich funkčního vybavení, systémy a prvky zajišťující zvýšení požární odolnosti stavebních konstrukcí nebo snížení hořlavosti stavebních hmot, požární přepážky a ucpávky). [14]

V rámci organizace provádí kontrolu dodržování podmínek požární bezpečnosti odborně způsobilá osoba v požární ochraně, která zároveň provádí i pravidelná školení zaměstnanců o požární ochraně. [14]

Samozřejmostí by měla být požární prevence všech zaměstnanců, která zahrnuje:

- udržování volných únikových cest,
- neponechávání elektrických spotřebičů v provozu bez dozoru,
- dodržování bezpečné vzdálenosti pro hořlavé materiály od zdrojů tepla,
- uniklé hořlavé kapaliny ihned zachytit vhodným sorbentem, který je zlikvidován uložením do předepsaných nádob,
- kontrolu hasicích přístrojů, zda jsou na správném místě a v provozuschopném stavu,
- obeznámení se s evakuačními plány pro případ mimořádné události. [11]

2.3.6 Informační bezpečnost

Komplexní ochrana informací v organizaci představuje systém s několika subsystemy – rovinami. Ty jsou následující:

- personální,
- technické řešení,
- metodologická a koncepční,
- uplatňování bezpečnostních postupů a opatření,
- bezpečnostně organizační, režimová a technologická,
- bezpečnostní informační audity. [8]

Při ochraně informací je nutné zdůraznit, že klíčovým faktorem jsou lidé, jejich nespolehlivost a možnost selhání. Další možností úniku informací jsou samotné technické systémy, které se v organizaci používají ke zpracování a následnému přenášení informací. [8]

V personální rovině se v ochraně informačních systémů jedná především o konkrétní události způsobené zaměstnanci. Organizace by měla všechny své zaměstnance upozornit na zachování mlčenlivosti o faktech, které by mohly poškodit dobré jméno podniku. [6]

V rovině režimové bezpečnosti je nutné vytvořit bezpečnostní pravidla pro nakládání s informacemi, daty a počítačovými systémy. Jedná se zejména o to:

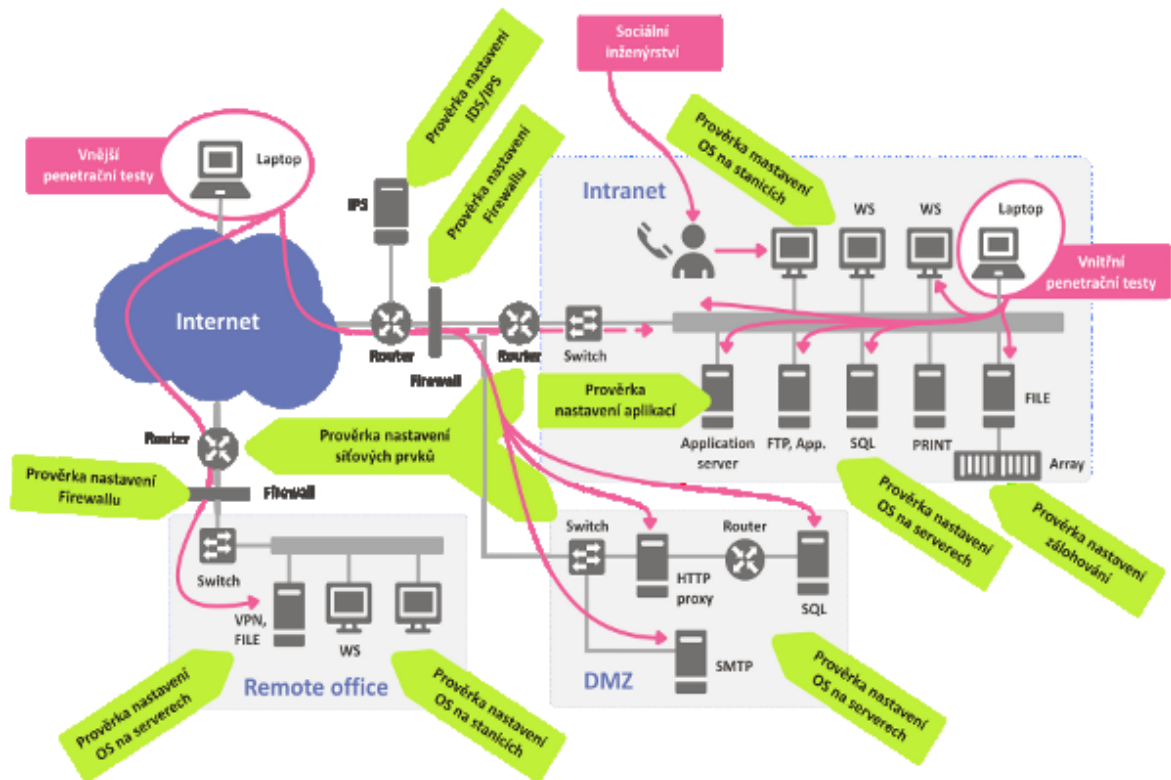
- stanovit, co je v rámci dané organizace považováno za důvěrné a utajované informace,
- vymezit okruh osob, které mohou s těmito důvěrnými informacemi pracovat,
- stanovit, jak bude s důvěrnými informacemi nakládáno a jak budou kontrolovány,
- jakým způsobem se budou ukládat datová média,
- plán pro případ mimořádných událostí apod.

Nestačí však pravidla pouze vytvořit, ale důsledně kontrolovat jejich dodržování. [8]

U bezpečnosti technických prostředků jde zejména o jejich samotný výběr a spolehlivost, kontrolu přístupu k nim, ochranu před elektromagnetickým zářením a elektrostatickou elektřinou.

Bezpečnost programových prostředků spočívá zvláště v ochraně proti virům, které mohou napadnout informační systém. Dále v ochraně proti zneužití, poškození či dokonce zničení softwarového vybavení. Taky by měl být kontrolován přístup do programů, na základě identifikace uživatelů a definovány pravomoci mezi uživateli. [8]

V informační bezpečnosti slouží k ověření a posouzení nynější úrovně odolnosti zkoumaného systému tzv. **penetrační test**. Jeho grafické znázornění můžeme vidět na obrázku č. 6. Je to pokus o průnik do informačního systému na žádost zákazníka. Jeho úkolem je odhalit co nejvíce možných děr a cest, které nejčastěji zneužívají hackeři k napadení systému. Tento vyžádaný útok má své pravidla a náležitosti a musí být v souladu s normami ČSN ISO/IEC TR 13335, ČSN ISO/IEC TR 17799 a ISO 27000. [1]



Obr. 6. Penetrační test v organizaci a jeho cíle [16]

K penetračnímu testování jsou využívány metody a nástroje manuálního i automatického charakteru, vždy je usilováno o to, co nejvíce se přiblížit reálnému napadení. [1]

2.4 Průběh auditu

Jednotlivé fáze BA, je možno vidět na obrázku č. 7. Auditní metodologie zahrnuje plánování, fázi přípravnou, realizační, vyhodnocovací a etapu následné kontroly. [7]



Obr. 7. Cyklus auditu [7]

2.4.1 Plánování

V praxi není nikde pevně stanoveno, v jakých časových intervalech má BA probíhat, záleží tedy na potřebách a požadavcích organizace. Pokud je organizační struktura firmy členitější, je výhodnější vykonávat audit průběžně kvůli přehledu o možných hrozbách a eventuálně včas reagovat adekvátním protiopatřením. V rámci plánování se taktéž stanovuje komplexnost auditu, na kterou oblast se zaměří, personální zabezpečení atd. Fázi plánování je třeba věnovat důkladnou přípravu, aby bylo předcházeno tomu, že rychle a povrchně naplánovaný BA neodhalí problémy systému. [6]

2.4.2 Příprava

Přípravnou fázi můžeme specifikovat v následujících bodech:

- na základě analýzy rizik je naprosto nezbytné definovat cíl BA,
- získávání bezpečnostních informací - využívají se jak zdroje vnější, tak především vnitřní, protože předmětem auditu je stav bezpečnosti uvnitř firmy,
- stanovení termínu a délky BA,
- určení členů auditorského týmu (zda bude audit proveden pracovníky bezpečnostního managementu nebo externí firmou). Tento tým se musí následně

s dostatečným předstihem obeznámit se všemi potřebnými dokumenty (to jsou např. organizační směrnice, zprávy z předešlých auditů, dokumenty k řízení procesů, záznamy o bezpečnostních problémech, předpisy o požární ochraně aj.) a oblastí, ve které bude provádět kontrolu,

- vypracování časového harmonogramu,
- zvolení vhodného postupu a techniky BA. [6]

2.4.3 Techniky auditorské práce

Auditor by měl vždy zvolit takový postup a rozhodovací metodu, aby dosáhl požadovaných výsledků. Podstatou je práce s informacemi, při vlastním posuzování musí auditor postupovat velmi opatrně, aby nedošlo ke špatnému zhodnocení a tím k ohrožení správnosti celého BA.

Jsou využívány následující metody:

- **porovnávání a ověřování** – obsah dokumentů je porovnán se skutečností,
- **rozhovor** – nejčastější metoda, auditor vede rozhovory se zaměstnanci, předem se stanoví otázky, aby zbytečnými dotazy nedocházelo k únikům informací,
- **pozorování** – jde o systematické sledování určitých činností, výsledkem je popis skutečností, ale i jejich vysvětlení,
- **šetření** – jedná se o aktivní vyhledávání informací v organizaci ze strany auditora, takto získané informace se srovnávají se stanovenými cíli v oblasti bezpečnosti organizace a zjišťují se případné rozdíly,
- dále se může jednat o **měření hodnot, testování, kontrolní výpočty** apod. Většinou se metody kombinují. [11]

2.4.4 Realizační fáze

Realizační fáze je zahájena vzájemným seznámením auditorů se zástupci auditovaného pracoviště. Následuje pohovor, při kterém jsou všichni zúčastnění obeznámeni s:

- cílem auditu,
- konkrétním místem, kde bude audit probíhat,
- personálním zajištěním a jejich pravomocemi,
- časem, v jakých hodinách bude BA vykonáván (ve dne, v noci, za provozu atd.). [6]

Na tomto setkání se většinou doladují poslední nezbytnosti mezi auditorem a vedoucími pracovníky daného úseku.

V dalším kroku sbírá auditor potřebné informace, zaznamenává si zjištění a objektivní důkazy – postup se odvíjí od řady faktorů, především záleží na zvolené metodě.

Analýzou zjištěných rozdílů od požadovaného stavu jsou pak krok za krokem odhalovány jednak příčiny nedostatků, tak i „silné stránky“ bezpečnostního systému podniku.

Realizační fáze je ukončena oficiálním závěrečným jednáním, při kterém je zhodnocena celková bezpečnost auditovaného místa, a následně je vypracována písemná zpráva. [6]

2.4.5 Zpracování závěrečné zprávy

Po ukončení jednotlivých fází BA je vyhotovena tzv. předběžná zpráva. Po seznámení s jejím obsahem je možné, aby se každá osoba, které se audit bezprostředně dotkl, k této zprávě vyjádřila. Je obvyklé, že si vrcholný management organizace stanoví lhůtu, po kterou je možné předběžnou zprávu připomínkovat, většinou to je patnáct až třicet dnů. Teprve po tomto období předá auditor zprávu závěrečnou. [6]

Závěrečná bezpečnostní zpráva je písemný dokument o provedeném BA a měla by současně obsahovat i návrh opatření. Skládá se z těchto částí:

- obsah dokumentu,
- seznam příloh zprávy,
- upřesnění použitých vnitropodnikových předpisů, právních a technických norem,
- seznam zkratk a pojmů, které se vyskytly v dokumentu,
- stanovený rozsah a cíl auditu,
- použité metody, postupy a jakým způsobem byly klasifikovány důkazy,
- stručná charakteristika firmy – oblast působení firmy, právní forma, vnitřní organizační struktura atd.,
- popis areálu, jednotlivých staveb a pracovišť z hlediska lokalizace apod.,
- popis konkrétního objektu, kterého se bude BA týkat,
- popis současného stavu a způsobu zabezpečení,
- identifikace hrozeb a analýza rizik,
- seznam silných a slabých míst,
- výrok, [6]

- návrh bezpečnostního opatření, který povede k odstranění nedostatků.

Je obvyklé, že na závěr auditor svou konečnou bezpečnostní zprávu prezentuje vedení firmy a tím se snaží své zjištěné výsledky obhájit. [6]

2.4.6 Vyhodnocení auditu a fáze následné kontroly

Vedení firmy by mělo po skončení auditu zhodnotit jeho přínosy, poučit se z výsledků BA a implementovat nápravná opatření k odstranění zjištěných nedostatků. Dalším důležitým krokem, který by měl nezbytně následovat, jsou pravidelné kontroly vedoucích pracovníků ve stanoveném časovém horizontu. Ti by měli dohlížet na činnosti, které byly v rámci auditu kontrolovány, zda dochází k odstranění neshod a případně navrhnout v rámci bezpečnostní politiky organizace jejich postupné zdokonalování. Pokud dochází v organizaci ke změně celé bezpečnostní politiky nebo je větší počet změn, je nutno vykonat po určitém čase následný audit. [6]

2.5 Shrnutí kapitoly

Ve druhé kapitole byl vysvětlen samotný pojem bezpečnostní audit, jaké jsou jeho cíle, možnosti dělení z různých hledisek, jednotlivé oblasti BA. Dále byly detailně popsány jednotlivé kroky BA a ty jsou následující: fáze plánování, přípravy, samotná realizace, vypracování závěrečné zprávy a následné vyhodnocení a kontrola.

3 CHARAKTERISTIKA DISTRIBUČNÍ FIRMY

Jelikož je bezpečnostní audit v praktické části diplomové práce proveden ve vybrané distribuční společnosti, je tato kapitola věnována obecné charakteristice distribučních společností.

3.1 Vymezení pojmů

Distribuce jako obor je součástí logistiky. V dnešním vyspělém tržním hospodářství může být úspěšná pouze ta firma, která se snaží uspokojit stále náročnější potřeby zákazníků zajímavou nabídkou nového, vysoce kvalitního zboží nebo služeb. Už nestačí pouze vyrobit nebo nakoupit hodnotné zboží či připravit služby, ale je třeba, aby bylo k dispozici se správnou kvalitou, u správného zákazníka, ve správném množství, na správném místě, ve správném okamžiku a to všechno s vynaložením přiměřených nákladů. Všechny zmíněné podmínky pomáhá řešit právě logistika. [18]

Jako vždy jednotná definice či názor neexistuje, nejvýstižněji se to podařilo formulovat Sixtovi J, na základě mnohaletých odborných i osobních zkušeností z hospodářské praxe: *„Logistika je řízení materiálního, informačního i finančního toku s ohledem na včasné splnění požadavků finálního zákazníka a s ohledem na nutnou tvorbu zisku v celém toku materiálu. Při plnění potřeb finálního zákazníka napomáhá již při vývoji výrobku, výběru vhodného dodavatele, odpovídajícím způsobem řízení vlastní realizace potřeby zákazníka (při výrobě výrobku), vhodným přemístěním požadovaného výrobku k zákazníkovi a v poslední řadě i zajištěním likvidace morálně i fyzicky zastaralého výrobku.“* [18, str. 25].

3.2 Cíle logistiky

Do podnikové strategie musí zapadnout strategie logistického systému podniku a logistické cíle musí podporovat hlavní cíl podniku. Cíle podnikové logistiky jsou následující:

- vychází z podnikové strategie a napomáhají je splňovat,
- musí být zabezpečena právní zájmy zákazníků na zboží a služby s požadovanou úrovní a to při minimalizaci celkových nákladů,
- zvyšování objemu prodeje, zkracování dodacích lhůt, zlepšování spolehlivosti a úplnosti dodávek,

- dalším cílem logistiky je minimalizace nákladů na skladové zásoby, dopravu, manipulaci a skladování. [18]

3.3 Distribuce výrobků

Jedno z nejdůležitějších rozhodnutí vrcholového managementu podniku se týká řešení otázky komu, a kde se budou výrobky prodávat. Dále jakým způsobem lze zajistit, aby výrobek byl nabízen na správném místě a ve správném okamžiku.

Výrobky se dostávají k zákazníkovi prostřednictvím tzv. **prodejních cest**. Je to souhrn prostředků a zprostředkovatelských článků, jejichž prostřednictvím přechází zboží od výrobce ke kupujícímu. Prodejní cesta funguje jako systém, který umožňuje plynulý fyzický tok zboží, jeho vlastnických práv, informací, stimulování prodeje a plateb za zboží. [19]

Prodejní cesty dělíme na:

- **přímé** - výrobce prodává své výrobky přímo koncovému zákazníkovi. Výrobce si tak musí sám zajistit obchodní, logistické i doplňkové funkce,
- **nepřímé** - je to taková cesta výrobku od výrobce k zákazníkovi, do které se zapojuje jeden či více mezičlánků – např. velkoobchod, maloobchod apod.

Každá z těchto cest má své výhody a nevýhody, v dnešní době je nejvíce využíváno cest nepřímých.

Jelikož vybraná společnost, ve které bude v praktické části diplomové práce proveden bezpečnostní audit, je **velkoobchodní síť**, bude dále specifikován pouze tento mezičlánek nepřímé distribuční cesty.

Firmy zabývající se velkoobchodní činností nakupují výrobky za účelem dalšího prodeje maloobchodním či jiným organizacím. Jejich specifikace je následující:

- přetváří úzký výrobní sortiment na široký sortiment obchodní,
- překlenuje časový nesoulad mezi výrobou a spotřebou,
- vytváří skladovou zásobu v takovém rozsahu, aby pružně vykrýval objednávky odběratelů,
- vytváří odběratelům obchodní úvěr a tím tak tvoří podmínky pro daleko větší prodej výrobků. Dodavatelům často platí dříve než maloobchod,
- přebírá riziko spojené s nákupem, dopravou a skladováním zboží,

- stimuluje prodej zboží jednotlivými nástroji stimulačního mixu, což je reklama, podpora prodeje, přímý marketing atd.,
- zajišťuje dopravu do maloobchodní sítě, což je z pohledu hustoty sítě pro výrobce téměř nemožné,
- poskytují výrobcům zpětné informace od zákazníků o konkurenci, cenách, zvláštních poptávkách, o nových výrobcích a taky o situaci v jiných oblastech. [20]

Více je oblast logistiky a distribuce zpracována v bakalářské práci Analýza rizik v distribuci. [21]

3.4 Shrnutí kapitoly

Tato kapitola byla věnována obecné charakteristice distribučních společností. Byl vymezen pojem logistika, dále cíle logistiky, přímé a nepřímé prodejní cesty a na závěr byla uvedena specifika distribuční společnosti.

II. PRAKTICKÁ ČÁST

4 SEZNÁMENÍ S AUDITOVANOU FIRMOU

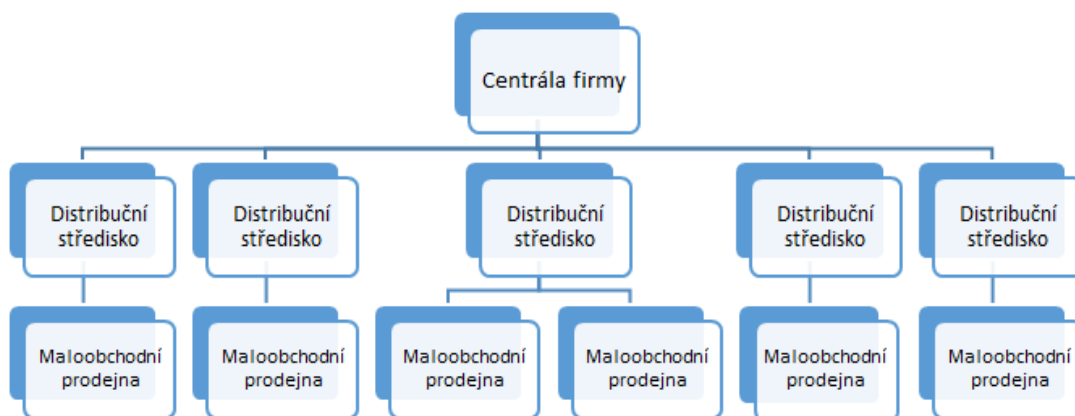
Pro svou diplomovou práci jsem si vybrala společnost, patří k největším velkoobchodním sítím nátěrových hmot a příslušenství v České republice (dále jen ČR). Tato kapitola je věnována charakteristice společnosti. V rámci ochrany firmy nebylo možné zveřejnit všechny informace.

4.1 Základní údaje o společnosti

Distribuční firma je akciovou společností a byla založena v roce 2000, k nejvýznamnější změně došlo v roce 2005, kdy se tato firma stala dceřinou společností českého výrobního podniku. To vedlo k zásadním změnám ve strategii obchodní politiky i celé koncepcie firmy, k finanční stabilitě a ke zvýšení konkurenceschopnosti na českém trhu. V době psaní diplomové práce zaměstnává společnost zhruba 140 zaměstnanců.

4.2 Organizační struktura

Organizační strukturu společnosti znázorňuje obrázek č. 8.



Obr. 8. Organizační struktura společnosti [zdroj vlastní]

Velkoobchodní společnost je řízena z centrály, kde sídlí vedení společnosti – majitelé velkoobchodu, generální ředitel, obchodní a finanční ředitel.

Distribuce výrobků probíhá z pěti velkoobchodních středisek a pokrývá celou ČR. V posledních letech se velkoobchod rozšířil i o síť vlastních maloprodejen.

4.3 Personální obsazení

Každé středisko je personálně obsazeno následovně:

- **vedoucí střediska** - řídí a zodpovídá za chod střediska, má na starosti manažersky – organizační oblast, rozhoduje převážně samostatně, pouze minimum věcí je řízeno centrálně. Každá oblast republiky je totiž něčím specifická, zákazníci mají jiné potřeby a nákupní návyky,
- **nákupčí** - zajišťuje nákup výrobků od dodavatelů a příjem zboží do skladu (ne fyzicky, pouze v informačním systému),
- **fakturantky** - přijímají zakázky od zákazníků, vystavují faktury (počet - většinou dvě),
- **skladníci** - fyzicky přejímají zboží, umisťují výrobky na skladové místo, vychystávají zákaznické objednávky (počet 3–6, podle velikosti střediska),
- **řidiči** - rozváží objednané zboží ke koncovým zákazníkům (počet 2–5, podle velikosti střediska),
- **prodavači na maloprodejnách** - pod jednotlivá střediska spadají vlastní maloobchodní prodejny, ty je zásobují zbožím, ale jinak jsou maloprodejny řízeny z centrály velkoobchodu (počet prodavačů 1–4, podle velikosti maloprodeje),
- **smluvní obchodní zástupci** - nejsou zaměstnanci firmy, na základě smlouvy o zprostředkování zajišťují podporu prodeje v maloobchodním segmentu, na území ČR takto působí dvanáct osob. Mezi jejich náplň práce patří pravidelná komunikace se zákazníkem a jeho osobní návštěva, předávání informací o pravidelných měsíčních slevách, o novinkách v sortimentu, sortimentní školení, technická podpora na prodejně, zajištění reklamy pro zákazníky atd.

4.4 Prodejní sortiment společnosti

Distribuční společnost má ve svém portfoliu výrobky z tuzemské i zahraniční produkce, sortiment čítá cca. 18 000 artiklů od zhruba padesáti dodavatelů.

Prodejní sortiment má následující skladbu – viz obrázek č. 9:

- barvy syntetické (na kov, dřevo, beton)
- barvy vodouředitelné (na kov, dřevo, beton, vnitřní malířské barvy, venkovní malířské barvy),

- barvy polyuretanové,
- barvy epoxidové,
- barvy nitrocelulózové,
- barvy epoxidové,
- spreje, tmely, lepidla,
- ředidla, tužidla, čističe, odstraňovače nátěrů,
- příslušenství (válečky, štětce, stříkací pistole, fólie, zakrývací pásy atd.).



Obr. 9. Prodejní sortiment [22][23][24]

4.5 Shrnutí kapitoly

V rámci této kapitoly je charakterizována distribuční společnost, ve které bude bezpečnostní audit proveden. Bylo zmíněno její personální zajištění, organizační struktura a samotný prodejní sortiment.

5 POPIS A CHARAKTERISTIKA AREÁLU

Cílem diplomové práce je provést BA v distribuční firmě. Jelikož se jedná o velký komplex, není možné v rámci této práce obsáhnout všechny činnosti a všechny střediska společnosti. Proto jsem se zaměřila na jeden z velkoobchodních skladů, který sídlí ve větším areálu. Jelikož stav bezpečnosti uvnitř firmy ovlivňuje i to, jakým způsobem je zajištěna bezpečnost z vnějšku, nejdříve popíši současný stav v tomto areálu.

5.1 Stručný popis areálu

Distribuční sklad se nachází v areálu na okraji města, v blízkosti velmi frekventované silnice. Areál je po celém obvodu oplocen kovovým plotem, pro vstup/výstup osob a vjezd/výjezd vozidel do areálu slouží jedna brána – viz obrázek č. 10. Hned za ní se nachází hlavní administrativní budova s vrátnicí. Ke vstupu do této budovy slouží jeden hlavní osobní vchod a další dva, které jsou využívány pouze minimálně. Vstup do budovy je povolen až po nahlášení svého jména zaměstnanci společnosti, který má oprávnění vpouštět do budovy – toto platí v době 6:00 až 14:00. Poté zajišťuje možnost vstupu do této budovy zaměstnanec bezpečnostní agentury, který zde vykonává fyzickou ostrahu. Lokalita není zajištěna kompletním poplachovým zabezpečovacím a tísňovým systémem, ani kamerovým systémem. V celém areálu je velká frekvence pohybu osob v pondělí až pátek a v době od 6:00 do 18:00.



Obr. 10. Vjezd do areálu [22]

Kromě budovy skladu distribuční společnosti, ve které bude proveden BA, sídlí v tomto areálu dalších šest firem. Některé z nich jsou ve stálém nájmu, jiné si budovy od majitelů areálu odkoupili. Jsou to firmy, které se zabývají opravou nákladních aut, výrobou plotů, kovovýrobou a velkoobchodní činností.

Pouze jedna firma má svou budovu samostatně oplocenu, zbývající budovy v areálu jsou volně stojící bez dodatečných plotů. Pracovní doba v těchto firmách se různí, v zimních měsících je to většinou 6:30–15:00, v letních měsících pracují zaměstnanci na směny od 5:00–20:00. Některé firmy mají nainstalován elektronický systém kontroly vstupu a kamerový systém.

5.2 Obvodová ochrana areálu

Jak již bylo výše zmíněno, celý areál je oplocen kovovým plotem, který je 1,5-2 m vysoký. Plot je napnutý a upevněný ke kovovým nebo betonovým sloupkům, které jsou zabetonovány do země. Různé druhy plotů jsou vidět na obrázcích č. 11 a č. 12. K vypnutí pletiva slouží napínací drát, který je připevněn ke sloupkům vázacím drátem. Pletivo je zavěšeno a zaháknuto v horní části napínacího drátu a k vypnutí pletiva slouží jeho střední a spodní část. Ke zvýšení ochrany před vniknutím je plot v některých místech rozšířen o 4 prameny ostnatého drátu a to ve vodorovné rovině. Tento ostnatý drát je připevněn opět vázacím drátem.



Obr. 11. Ukázka plotu s ostnatým drátem [22]



Obr. 12. Ukázka plotu z jiné části areálu [22]

V rámci zvýšení ochrany areálu není bohužel instalován žádný kamerový systém, který by vhodně doplňoval fyzickou ostrahu.

5.3 Kontrolní propustková služba

Pro vstup/výstup osob a vjezd/výjezd vozidel do areálu slouží jedna brána. Tato brána je otevřena v době 5:30–20:00. Vrátnice se nachází v hlavní administrativní budově společnosti, která je vlastníkem areálu. Tuto budovu vidíme na obrázku č. 13.



Obr. 13. Vrátnice v administrativní budově [22]

Po dobu, kdy je brána otevřená, je vjezd do areálu nekontrolován, mohou vjíždět/vyjíždět jakékoliv osobní nebo nákladní auta nebo taky vstupovat/vystupovat jakékoliv osoby.

Do areálu vjíždějí nejčastěji osobními auty zaměstnanci jednotlivých firem, kteří parkují na vyhrazených parkovištích u firem, dále vlastní nákladní auta, která odváží zboží ze skladů a v poslední řadě externí nákladní auta a kamiony, která slouží jako zásobování distribučních skladů. Řidiči nehlásí na vrátnici své jméno ani SPZ vozidla, neprobíhá kontrola nákladu.

Co se týká pohybu osob v areálu, můžeme je rozdělit do těchto kategorií:

- samotní zaměstnanci firem,
- zákazníci – ať už občasní, nebo stálí,
- řidiči nákladních aut, kamionů,
- osoby, které vstupují do areálu za účelem návštěvy konkrétní firmy z důvodu osobního jednání (např. obchodní zástupci z dodavatelských firem).

Pohyb osob po areálu není nikterak omezován, lidé se nemusí identifikovat na vrátnici, při východu z areálu neprobíhá osobní kontrola.

Po uzavření brány je režim jiný, vstup do areálu je zaměstnancem bezpečnostní agentury umožněn pouze těm osobám, které pracují v některé z firem zde sídlících, a to až na základě identifikace. Strážný si zaznamená potřebné údaje do deníku a jsou to následující:

- jméno a příjmení osoby požadující vstup do areálu,
- název společnosti, ve které pracuje,
- pokud přijede osoba vozidlem, tak SPZ vozidla,
- datum a čas příchodu do areálu,
- datum a čas odchodu z areálu.

Při opouštění osoby areálu nedochází k osobní kontrole ani ke kontrole případného nákladu.

Záznamy v deníku slouží pro zpětnou kontrolu v případě potřeby pro bezpečnostní agenturu nebo majitele firmy, do které osoba vstupovala, a tato firma není vybavena elektronickým systémem kontroly vstupu osob.

5.4 Fyzická ostraha

V rámci areálu je fyzická ostraha zabezpečována soukromou bezpečnostní agenturou, jejíž název majitel nepovolil zveřejnit. Tato služba je zajišťována na základě smlouvy o poskytování soukromých bezpečnostních služeb, objednatelem je majitel areálu a vztahuje se na všechny firmy zde sídlící, bez rozdílu, zda jsou v nájmu nebo budovy vlastní.

Zaměstnanci soukromé bezpečnostní agentury vykonávají v rámci areálu následující činnosti:

- kontrolní propustkovou službu ve vymezeném čase,
- zajišťování bezpečnosti v celém areálu,
- kontrolní pochůzkovou činnost,
- klíčový režim pro vybrané firmy,
- realizaci zásahu v případě mimořádné události,
- požární hlídku a v případě potřeby asistenci,
- při zjištění skutečného narušení objektu ihned vyrozumí příslušné obvodní oddělení Policie ČR.

Dle strážního řádu firmy mají strážní při plnění svých úkolů stejná práva a povinnosti, jako by měli vlastní zaměstnanci majitele areálu.

Fyzická ostraha probíhá nepřetržitě pouze o víkendech, ve dnech od pondělí do pátku v dohodnutém čase, jak je vidět v tabulce č. 2. V těchto směnách se střídají celkem čtyři zaměstnanci soukromé bezpečnostní agentury.

Tab. 2. Pracovní doba strážných [14]

Pracovní dny	Zahájení směny	Ukončení směny
Pondělí - Pátek	14:00	06:00
Sobota - Neděle ranní směna	06:00	18:00
Sobota - Neděle noční směna	18:00	06:00

Kontrolní pochůzkovou činnost po areále vykonává strážný každé dvě hodiny.

Při rozhovoru s vedoucím areálu bylo zjištěno, že v uplynulých pěti letech nebylo evidováno žádné vniknutí do střežených objektů ani nedošlo k úmyslnému poškození majetku.

5.5 Shrnutí kapitoly

V rámci této kapitoly byl stručně charakterizován areál, ve kterém sídlí vybraná distribuční společnost. Bylo popsáno, jak zde probíhá kontrolní propustková služba, fyzická ostraha i jakým způsobem je zabezpečen celý areál.

6 POPIS A CHARAKTERISTIKA VYBRANÉHO OBJEKTU

Tato kapitola je zaměřena na stručnou charakteristiku objektu distribučního skladu a dále je popsán současný stav jednotlivých oblastí bezpečnosti ve firmě.

6.1 Charakteristika objektu

Objekt distribučního skladu můžeme provozně rozdělit na skladovací část a administrativní část. Je to přízemní volně stojící zděná budova, která byla postavena v sedmdesátých letech 20. století. Výrobky jsou skladovány na ploše 2010 m². Sklad je provozně členěn na dva prostory skladu – nezateplený a zateplený. Tyto skladovací prostory jsou od sebe odděleny požární stěnou. Podlaha ve skladu je nepropustná a odolná proti chemickým účinkům hořlavých kapalin. Vytápění skladovacích prostorů zajišťují tři průmyslové teplovzdušné plynové jednotky zn. ROBUR F1 – viz obrázek č. 14.



Obr. 14. Průmyslová teplovzdušná plynová jednotka ROBUR F1 [22]

Součástí budovy je nákladová rampa – viz obrázek č. 15, která je využívána řidiči k naložení zboží při expedici zakázek ze skladu a taky pro vyložení zboží od dodavatelů. V administrativní části budovy se nachází kanceláře fakturantek a vedoucího pracovníka, sociální zařízení a šatny zaměstnanců.



Obr. 15. Nákladová rampa [22]

Objekt skladu nemá své vlastní oplocení, je tedy volně přístupný, oplocen je pouze ze zadní strany budovy plotem, který patří areálu.

V době psaní diplomové práce pracuje na středisku dvacet zaměstnanců. Ve firmě se nepracuje na směny, pracovní doba je od pondělí do pátku v měsících březen–září od 5:30 do 15:30 a měsících říjen–únor od 6:30 do 15:00.

Velkoobchodní společnost není vlastníkem budovy, na základě nájemní smlouvy je v dlouhodobém nájmu.

6.2 Plášt'ová ochrana

Vstup do prostor kanceláří je umožněn plastovými dveřmi se skleněnou výplní. Dveře jsou opatřeny bezpečnostní vložkou typu R1. Skleněná výplň dveří ani kancelářská plastová okna nejsou chráněna kovovými mřížemi. Do skladovacích prostor se vstupuje třemi těžkými kovovými vraty, která jsou uzamykatelná na visací kovové zámky – viz obrázek č. 16.



Obr. 16. Zámek visací 50mm

kovový [25]

Ve skladě jsou okna umístěna ve výšce cca tři metry. Je to ocelový rám, který je zasklen drátosklem, členěný na několik menších tabulek, jak je vidět na obrázku č. 17.



Obr. 17. Okna do skladu [22]

6.3 Klíčový režim

Hlavní klíče od budovy má vedoucí pracovník a další klíč je uložen na vrátnici, ke kterému mají přístup všichni zaměstnanci firmy. Klíč vyzvedává na vrátnici ten, který se dostaví jako první do zaměstnání. Strážný si vede záznam do deníku, kde si zapisuje datum vydání klíče, jméno a příjmení zaměstnance a jeho podpis. Při vracení klíče na vrátnici není požadován od zaměstnanců již žádný údaj ani podpis, strážný si sám zapíše čas vrácení klíče.

Ve firmě není vypracována obecná směrnice, která by jasně definovala rozsah klíčového režimu. Platí pouze nepsané pravidlo, že vedoucí pracovník má klíče od všech vstupů do budovy a přístup v kteroukoliv dobu. Zaměstnanci mohou vstupovat do budovy pouze v pracovní dobu a mimo tuto dobu nebo o víkendu pouze v mimořádném případě po předchozí dohodě s vedoucím pracovníkem (např. v letních měsících se někdy stává, že dodavatel nestíhá termíny dodávek, takže zboží přiveze i v sobotu dopoledne a skladník přijede zboží přijmout). Vedoucí střediska si může ověřit toto mimořádné vydání klíče právě v záznamu na vrátnici.

6.4 Požární ochrana

Jelikož se vybraná distribuční společnost zabývá prodejem nátěrových hmot, ředidel a rozpouštědel a uskladňované množství hořlavých kapalin (dále jen HK) je velké, je věnována požární ochraně (dále jen PO) značná pozornost.

Požární nebezpečí hrozí především z těchto důvodů:

- velké množství hořlavých kapalin na jednom místě,
- v jednom prostoru se vyskytují nebezpečné látky, které jsou klasifikovány jako oxidující, extrémně hořlavé a vysoce hořlavé,
- porušení podmínek pro bezpečný pohyb osob ve skladě,
- nedodržování požární prevence a povinností ze strany zaměstnanců.

Aby požární nebezpečí bylo minimalizováno, jsou barvy a HK ve skladě uloženy v originálních přepravních obalech – v plechovkách různého objemu nebo v 200 litrových sudech - a nedochází k přečerpávání nebo k přelévání těchto HK. Při jejich následném vyskladňování se provádí opětovná kontrola neporušenosti obalu. Dále je stanoveno maximální skladované množství HK a to 40 000 litrů, z toho je nejvýše přípustné množství HK I. a II. třídy nebezpečnosti 10 000 litrů. Kvůli velkým pohybům na skladě je momentální skutečný stav těchto HK zjistitelný u vedoucího střediska.

6.4.1 Technická zpráva požární ochrany a požární řád.

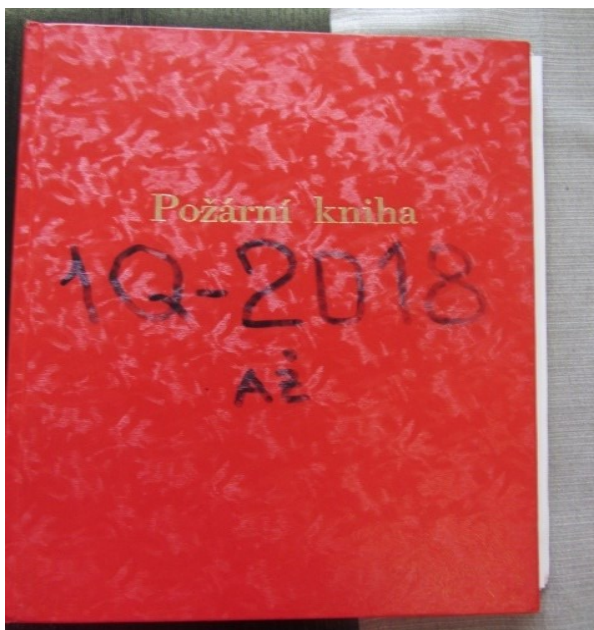
Pro sklad je vypracována technická zpráva požární ochrany a požární řád.

Tato **technická zpráva** posuzuje sklad z hlediska požární bezpečnosti a definuje požadavky na konstrukci a provoz skladu. Byly v ní použity tyto normy:

- ČSN 73 0824 výhřevnost hořlavých látek,
- ČSN 73 0804 výrobní objekty,
- ČSN 73 0821 požární odolnost stavebních konstrukcí,
- ČSN 73 0873 požární vodovody,
- ČSN 65 0201 HK – provozovny a sklady.

Požární řád na technickou zprávu požární ochrany navazuje a upřesňuje provoz skladu a manipulaci s HK z požárního hlediska.

V rámci požární ochrany spolupracuje firma na základě smlouvy s externí odborně způsobilou osobou v PO, která provádí 1 x za měsíc kontrolu dodržování podmínek požární bezpečnosti. O kontrole je proveden zápis do požární knihy – viz obrázek č. 18, kde se zaznamenávají zjištěné nedostatky, návrh na odstranění závad i s termínem nápravy. Po odstranění závady je potřeba zapsat, jakým způsobem to bylo provedeno, kdy a kdo ji odstranil.



Obr. 18. Požární kniha [22]

Budova skladuje řádně označena dle požárního řádu stanovenými bezpečnostními tabulkami - viz obr. 19.



Obr. 19. Označení skladu bezpečnostními tabulkami [22]

Pro přehlednost jsou v tabulce č. 3 uvedeny všechny výstražné a bezpečnostní tabulky, které jsou umístěny v prostorách velkoobchodu.

Tab. 3. Přehled o umístění výstražných a bezpečnostních tabulek [14]

Místo	Druh tabulky	Počet kusů
Sklad - vstupní vrata	Nepovolaným vstup zakázán	1
	Zákaz kouření a manipulace s ohněm	1
	Sklad HK - Nebezpečí požáru hořlavých kapalin	1
Sklad uvnitř	Prázdné přepravní obaly	2
	Plné přepravní obaly	2
	Hasicí přístroje	3
	Hydrant	2
Sklad uvnitř - zadní	Hořlavá kapalina I. a IV. Třídy nebezpečnosti	1
Hlavní vypínač elektrické energie	Čtyř-tabulka Pozor - elektrické zařízení, Hlavní vypínač, Vypni v nebezpečí, Nehas vodou ani pěnovými přístroji!	1

Jak už bylo výše zmíněno, skladovací prostory jsou od sebe odděleny požární stěnou, kterou tvoří sendvičová stěna CETRIS tloušťka 16 mm – vzduchová mezera 75 mm – deska CETRIS tloušťka 16 mm. Podlaha ve skladu je nepropustná a opatřená nátěrem odolným proti chemickým účinkům hořlavých kapalin. Nepropustná podlaha, zvýšený práh a sokl, který je 5cm vysoký, totiž tvoří havarijní jímku, která slouží pro zadržení při případném úniku HK. Sklad je odvětráván ventilátory v provedení SNV 2, které zajišťují dvojnásobnou výměnu vzduchu za hodinu.

6.4.2 Věcné prostředky požární ochrany

Pro zásah při mimořádné události jsou nejen prostory skladu, ale i administrativní část budovy vybaveny věcnými prostředky požární ochrany. V budovách je umístěno celkem

čtrnáct **přenosných hasicích přístrojů**, z toho je dvanáct práškových a dva jsou sněhové. Pro větší přehlednost je zpracována tabulka č. 4.

Tab. 4. Přehled přenosných hasicích přístrojů [22]

Místo umístění	Druh přenosného hasicího přístroje	Počet
Skład - rampa	Práškový – 6 kg	1
Skład nezateplený - u hydrantu	Práškový – 6 kg	5
Skład zateplený - u hydrantu	Práškový – 6 kg	4
Skład zateplený - u hydrantu	Sněhový – 5 kg	1
Skład zateplený - u nabíječky vozíku	Práškový – 6 kg	1
Administrativní část - u rozvodny	Sněhový – 5 kg	1
Administrativní část - chodba	Práškový – 6 kg	1

Nejvíce je v budovách využíván práškový hasicí přístroj – viz obrázek č. 20, který se používá i na elektrická zařízení. Kontrola těchto přístrojů probíhá 1 x za rok revizním požárním technikem, ten hasicí přístroj opatří samolepkou o této informaci. Tlaková zkouška probíhá 1 x za 5 let a i tato informace je vylepena na hasicím přístroji.

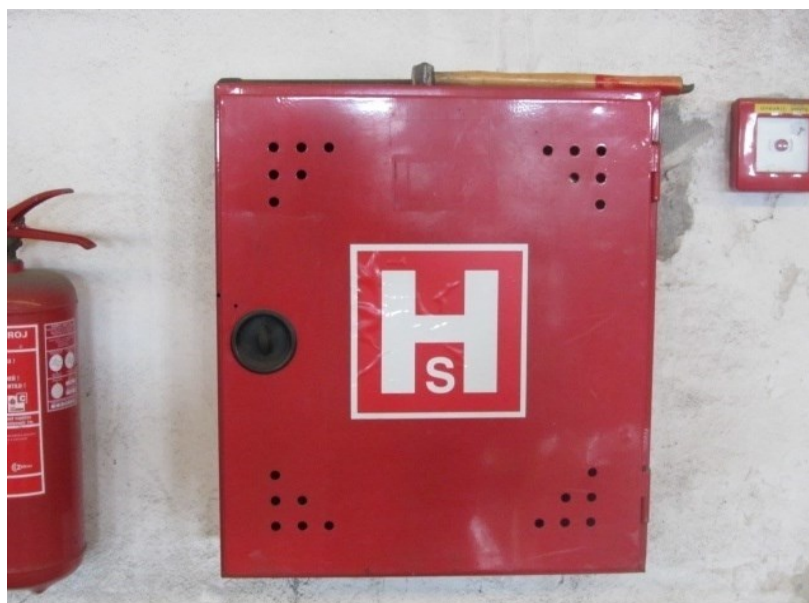


Obr. 20. Práškové hasicí přístroje v nezatepleném skladu [22]

Ve stejných intervalech probíhají kontroly i tlakové zkoušky u sněhových hasicích přístrojů. Taktéž jsou opatřeny náležitými samolepkami.

6.4.3 Požárně bezpečnostní zařízení

Vnější požární voda pro první zásah v případě požáru je zajištěna z podzemního **požárního hydrantu** vodovodu v rámci areálu. Ve skladě jsou umístěny dva nástěnné hydranty typu C 52, jeden se nachází v zateplené části a druhý v nezateplené. Jeden z hydrantů je vidět na obrázku č. 21.



Obr. 21. Požární hydrant [22]

Přívod vody do systému je řešen jako suchovod s napouštěním vody přes klapku se servopohonem. Ovládání hadicového systému (dále jen HS) je standardní. Před použitím se HS zavodní tlačítkem umístěným na ovládací skřínce u HS. Po použití HS se pomocí solenoidového ventilu provede odvodnění přívodního potrubí a HS, dále se provede znovunastavení klapky ovládané servopohonem. Ventil a klapka jsou umístěny na přívodním potrubí v prostoru vodovodní šachty pod podlahou kanceláře fakturantek. Ovládací skříňka, která je vidět na obrázku č. 22, se nachází taktéž v této kanceláři.



Obr. 22. Ovládací skříňka HS [22]

6.4.4 Školení zaměstnanců a prevence v PO

Pravidelná školení zaměstnanců ohledně PO provádí rovněž externí odborně způsobilá osoba v PO. Součástí školení je i praktický nácvik požárního zásahu při požáru. Tato školení probíhají v následujících intervalech – viz tabulka č. 5. O školení je proveden záznam s podpisy všech zúčastněných.

Tab. 5. Intervaly školení zaměstnanců o PO [14]

Pracovní zařazení	Interval školení
Vedoucí střediska	1 x za 2 roky
Skladník, řidič, fakturantky	1x za rok

V rámci prevence PO je ve velkoobchodním skladu zvolena požární preventivní hlídka. Tato hlídka má pět členů - všichni skladníci, a každý člen má stanovený svůj úkol v rámci prevence i při případném vzniku požáru. Tyto úkoly jsou zaznamenány do tabulky č. 6.

Tab. 6. Povinnosti členů požární preventivní hlídky [14]

Členové hlídky	Úkoly na úseku prevence	Úkoly při vzniku požáru
Velitel hlídky	Kontroluje dodržování požárního řádu skladu a upozorňuje na případné závady z hlediska PO	Řídí činnost požární hlídky při zásahu, vyhlásí pro ostatní požární poplach, oznamuje požár na ohlašovnu požárů, spolupracuje se zasahující jednotkou.
Člen hlídky č. 1	Kontroluje přístupnost k hlavním vypínačům elektrické energie. Dohlíží na trvalou průchodnost únikových cest a východů.	Provádí prvotní zásah dle pokynů velitele hlídky. Při požáru zasahuje práškovým hasicím přístrojem, popř. zasahuje pomocí nástěnného hydrantu.
Člen hlídky č. 2, 3	Kontroluje průběh nabíjení motorových vozíků.	Provádí prvotní zásah dle pokynů velitele hlídky. Při požáru zasahuje práškovým hasicím přístrojem, popř. zasahuje pomocí nástěnného hydrantu.

Dále je ve firmě zpracována požární poplachová směrnice, která je vyvěšena v každé místnosti budovy zároveň i s požárním řádem.

6.5 Bezpečnost a ochrana zdraví při práci

Distribuční společnost nezaměstnává svého bezpečnostního technika, nýbrž i v rámci oblasti BOZP spolupracuje s externí osobou odborně způsobilou v BOZP. Tato osoba zajišťuje pro firmu následující úkony:

- zajišťuje vstupní školení pro nové zaměstnance,
- provádí průběžné školení BOZP u všech pracovníků,
- 1 x za měsíc kontroluje pracoviště a vedoucího střediska upozorní na případné nedostatky,
- kontroluje vybavení lékárničky,
- poskytuje konzultace po telefonu v případě potřeby,

- v rámci případné změny bezpečnostních podmínek ve firmě vytvoří bezpečnostní opatření.

Vedoucí pracovník je školen 1 x za 3 roky, u ostatních zaměstnanců probíhá školení každoročně. Znalosti jsou ověřeny testem, o školení je proveden záznam s podpisy všech zúčastněných zaměstnanců.

Společnost má zpracovaný Místní provozní řád skladu hořlavých kapalin i směrnici BOZP, vše je uloženo u vedoucího pracovníka.

Vstupní prohlídky nových zaměstnanců i jiné preventivní prohlídky probíhají u smluvního lékaře pro pracovních lékařskou službu.

Na základě vyhodnocení rizik, pracovních činností a taky konkrétních podmínek na jednotlivých pracovištích jsou zaměstnancům poskytovány stanovené osobní ochranné pracovní pomůcky (dále jen OOPP), mycí, čistící a dezinfekční prostředky.

Seznam poskytovaných OOPP dle druhu pracovního zařazení a životnost OOPP je zpracován do tabulky č. 7. Životnost OOPP je teoretická, při jakémkoliv poškození či zničení OOPP je zaměstnanec povinen toto nahlásit a je mu poskytnuta nová.

Tab. 7. Seznam poskytovaných OOPP dle druhu pracovních činností a jejich životnost [14]

Druh pracovních činností	Druh OOPP	Životnost OOPP v měsících
Skladník	Ochranná přilba	1x při nástupu, dále dle potřeby
	Čepice zimní	60
	Pracovní rukavice	12
	Antistatické pracovní boty	24
	Kabát prošívaný	36
	Plášť do deště	48
	Pracovní oděv	12
	Ručník	6

Řidič nákladního auta	Výstražná vesta	48
	Zateplená vesta	48
	Pracovní obuv	24
	Pracovní oděv	24
	Pracovní rukavice	12
	Ručník	6

Veškeré poskytnuté prostředky jsou zapsány do evidenčního listu – viz tabulka č. 8, který má každý zaměstnanec.

Tab. 8. Evidenční list pro poskytování OOPP [14]

Název firmy	Středisko:			
Jméno zaměstnance:	Profese:			
Seznam OOPP:	Datum vydání	Podpis	Datum vrácení	Podpis

Zaměstnanec potvrdí převzetí svým podpisem. Pravidelnou kontrolu používání OOPP zaměstnanci má na starosti vedoucí střediska.

Pro případ náhodného úniku HK je sklad vybaven dostatečným množstvím sorbentů, havarijních souprav a kanalizačních ucpávek.

Společnost plní zákonnou povinnost vést dokumentaci o kontrolách a revizích elektrických spotřebičů, elektrických strojů, plynových zařízení, hromosvodu a zajišťovat provádění těchto kontrol, zkoušek či revizí. V případě zjištěných závad se odstraňují v co kratším čase.

6.6 Informační bezpečnost

Bezpečnost informačních systémů a informací je jedna z nejdůležitějších oblastí bezpečnosti a zároveň jedna z nejrizikovějších oblastí ochrany každé firmy. Stávající stav v této oblasti je popsán pouze částečně, protože serverovna a oddělení informačních technologií se nachází mimo budovu distribuční společnosti, kde mi nebyl umožněn vstup ani přístup ke všem požadovaným informacím.

6.6.1 Firemní informační systém

Z pohledu informačního systému byl pro firmu zásadní rok 2010. Distribuční společnost je totiž součástí skupiny několika firem, postupné rozrůstání skupiny a nejednotnost informačních systémů (dále jen IS) přimělo majitele k důležitému rozhodnutí. Jelikož měla každá firma svůj IS, které nebylo možné navzájem propojit, byl do všech společností napříč skupinou implementován jednotný IS. Při výběrovém řízení vhodného IS byly požadavky na nový systém velmi náročné, protože musely splňovat kritéria jak pro výrobní podnik, tak pro obchodní společnost. Přes počáteční obtíže po implementaci bylo nakonec toto rozhodnutí podle mého názoru správné, práce se zrychlila a zpřehlednila, denní výstupy pro majitele firmy jsou jednotné a došlo k úsporám provozních nákladů. Další výhodou je to, pokud by došlo k situaci, že se některý zaměstnanec přesune do jiné firmy v rámci skupiny, je ihned schopen pracovat s IS bez dalšího zaškolování.

Práva a přístup do IS je zřízen od pracovníků oddělení informačních technologií (dále jen IT), uživatelé se přihlašují pomocí svého uživatelského jména a univerzálního hesla. Toto univerzální heslo je potřeba při prvotním přihlášení do programu změnit. Heslo může mít minimálně pět znaků a maximálně deset znaků. Obměna hesel probíhá každé tři měsíce.

Co se týká práv v IS, ty jsou zaměstnancům omezeny na základě principu „nutná potřeba k práci“, tzn., že každý může pracovat pouze ve funkcích, které souvisí s oblastí jeho práce – např. nákupčí má povoleny všechny funkce spojené s nákupem, fakturantky s prodejem atd.

6.6.2 IT oddělení

S implementací jednotného systému došlo i k další změně a to v IT oddělení. Nyní nemá distribuční společnost své vlastní IT oddělení, všechno spadá pod kompetenci mateřské společnosti, která sídlí mimo velkoobchodní společnost.

V případě potřeby se problémy řeší přes vzdálený přístup TeamViewer, pracovník IT se během několika sekund připojí na libovolné zařízení a problém odstraní.

Pracovníci IT oddělení zajišťují následující:

- zřizují práva a přístupy do jednotlivých počítačů i IS,
- nakupují a instalují hardwarové zařízení dle potřeby,
- kontrolují obměnu hesel,
- zajišťují potřebné aktualizace programů,
- provádějí zálohu dat,
- upravují a zdokonalují IS dle potřeb firmy.

Kvůli potenciální ztrátě dat probíhá jejich pravidelná záloha a to vždy jednou denně v určité noční hodině.

V oddělení IT se nachází i hlavní servery, které jsou umístěny v jedné kanceláři tohoto oddělení. Tato kancelář je řádně označena a vstup je povolen pouze pracovníkům IT a uklízečkám. Místnost je klimatizovaná, teplota je zde nastavena na 14 – 17 °C. Dále je vybavena hlásiči, které reagují na oheň a kouř a taky na změnu teploty v případě poruchy klimatizace. Kvůli neočekávanému výpadku elektrického proudu je celá serverovna napojena na záložní UPS.

6.6.3 Pracovní stanice uživatelů

Jedna uživatelská stanice se nachází ve skladě a zbývající v administrativní části budovy. Ve skladě je počítač (dále jen PC) vybaven pouze programem k míchacímu zařízení a základními programy. K počítači je připojena tiskárna pro tisk etiket.

PC i tiskárny v kancelářích prošly před rokem obměnou, nové počítače jsou většinou od firmy Dell. Jsou vybaveny těmito programy:

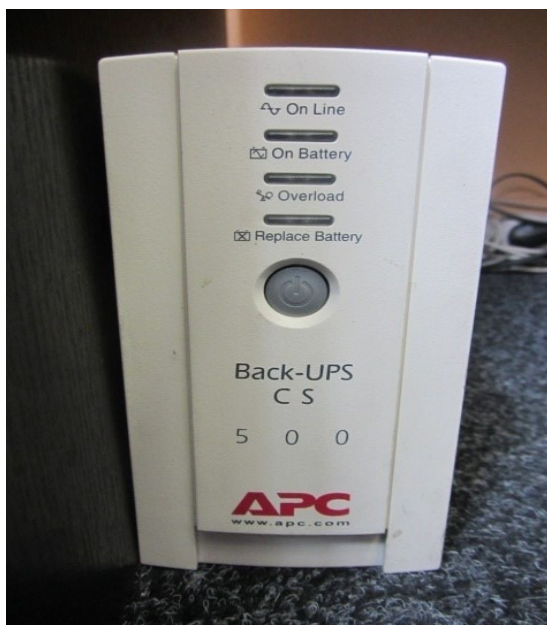
- Windows 7,
- Microsoft Office 2007,
- Internet Explorer 7
- Google Chrome,
- Pošta MS Outlook 2007,
- Adobe Reader,
- TeamViewer,

- program k míchacímu zařízení,
- program pro zaslání objednávek od zákazníků,
- program pro zpracování inventur a další.

Jako ochrana před viry, spyware a malware slouží na všech počítačích program Eset Endpoint Security 6.

Všechny zjištěné aplikace byly pokryty řádnou licencí.

Každá pracovní stanice je kvůli nenadálému výpadku elektrického proudu napojena na záložní UPS značky APC Back – UPS 500, s výkonem 500 VA – viz obrázek č. 23.



Obr. 23. Záložní zdroj k PC [22]

Všechny počítače jsou napojeny na internet, jednak kvůli firemnímu IS, objednávkovému systému i míchacímu systému.

6.7 Shrnutí kapitoly

V této kapitole je blíže charakterizován objekt distribuční společnosti a je popsán současný stav plášťové ochrany, klíčového režimu ve firmě, požární ochrany, BOZP a taky informační bezpečnosti.

7 BEZPEČNOSTNÍ AUDIT

Provedení bezpečnostního auditu v konkrétní společnosti není rutinní vyplňování předem nadepsaných tabulek nebo odškrtnutí v již napsaném seznamu. Každá firma je svým způsobem originál a má své specifické požadavky a potřeby. Není na místě se přesně držet norem, protože by se mohlo stát, že provedený audit bude spíše kontraproduktivní soubor pravidel než jakýsi doklad toho, na jakém stupni se bezpečnost ve firmě skutečně nachází.

7.1 Zaměření a cíle auditu

Cílem je provést interní bezpečnostní audit v distribuční firmě.

Tento audit je zaměřen na posouzení stávající bezpečnostní situace ve firmě a je postupováno následovně:

- prohlídka a analýza současného stavu,
- analýza dokumentace a vnitropodnikových směrnic souvisejících s bezpečností,
- analýza rizik,
- stanovit závěr auditu,
- na základě zjištěných výsledků navrhnout opatření, která budou bezpečnostní rizika minimalizovat, a to povede k dalšímu zvýšení bezpečnosti ve všech jejich oblastech.

7.2 Vstupní informace

Bezpečnostní audit je proveden v následujících oblastech:

- **obvodová ochrana areálu** – oplocení, brána, bezpečnostní prvky,
- **kontrolní propustková služba** – režim vrátnice, pohyb osob a aut po areálu,
- **fyzická ostraha** – náplň práce, pracovní doba, statistika vniknutí do objektů,
- **plášťová ochrana objektu distribučního skladu** – zabezpečení dveří, vrat, oken, technické prvky,
- **klíčový režim firmy** – směrnice, klíčový režim,
- **požární ochrana** – směrnice pro PO, věcné prostředky požární ochrany, požárně bezpečnostní zařízení, školení zaměstnanců v PO,
- **oblast BOZP** – směrnice pro BOZP, školení, poskytování OOPP, lékařské preventivní prohlídky,

- **informační bezpečnost** – směrnice, firemní IS, ochrana dat, práva a přístupy zaměstnanců do IS, antivirový program.

Během auditu byly prověřeny **dokumenty a interní směrnice** uvedené tabulce č. 9.

Tab. 9. Seznam prověřených dokumentů a interních směrnic [14]

Auditovaná oblast bezpečnosti	Název dokumentu nebo interní směrnice
Kontrolní propustková služba	Deník pro evidenci osob
Fyzická ostraha	Strážní řád bezpečnostní agentury
Klíčový režim	Deník pro klíčový režim
Požární ochrana	Technická zpráva požární ochrany
	Požární řád
	Požární kniha
	Smlouva s odborně způsobilou osobou v PO
	Záznam o školení zaměstnanců v PO
	Protokol o pravidelné kontrole hasicích přístrojů a hydrantů
	Požární poplachová směrnice
BOZP	Směrnice BOZP
	Místní provozní řád skladu hořlavých kapalin
	Pracovní smlouvy zaměstnanců
	Dohoda o provedení činnosti
	Protokol o pravidelné prohlídce teplovzdušných agregátů Robur
	Technická zpráva o revizi plynového zařízení
	Technická zpráva o kontrole plynového zařízení
	Zpráva o revizi elektrického zařízení

	Zpráva o revizi elektrické instalace strojního zařízení
	Zpráva o revizi ochrany před bleskem
	Zpráva o revizi ovládací skříňky HS
	Evidenční listy o předávání OOPP
	Smlouva s lékařem o pracovně-lékařské službě
	Smlouva s odborně způsobilou osobou v BOZP
	Lékařské posudky o zdravotní způsobilosti k práci
	Záznam o školení BOZP
	Záznam o školení řidičů
	Potvrzení o absolvování pravidelného školení dle zákona 247/2000 Sb., §48 odst. 2

7.3 Analýza současného stavu

Popis současného stavu jednotlivých auditovaných oblastí byl proveden v předešlých kapitolách diplomové práce a to následovně – viz tabulka č. 10.

Tab. 10. Přehled o provedení analýzy auditovaných oblastí [14]

Auditovaná oblast	Číslo kapitoly
Obvodová ochrana areálu	5
Kontrolní propustková služba	5
Fyzická ostraha	5
Plášťová ochrana	6
Klíčový režim	6
PO	6
BOZP	6
Informační bezpečnost	6

7.4 Analýza rizik

Po analýze současného stavu byly provedeny jednotlivé kroky analýzy rizik.

7.4.1 Identifikace aktiv

Ve firmě je nutné ochraňovat následující tři skupiny aktiv:

- hmotný a nehmotný majetek,
- fyzické osoby,
- informace.

7.4.2 Identifikace hrozeb pomocí metody „Kontrolní seznam“

Po zhodnocení současného stavu bezpečnosti v jednotlivých sekcích ve společnosti a po porovnání s poskytnutou dokumentací byly identifikovány bezpečnostní hrozby pomocí metody Kontrolní seznam – viz tabulka č. 11.

Tab. 11. Kontrolní seznam [14]

Otázka	ANO	NE
Je areál firmy oplocený?	X	
Je plot v dobrém technickém stavu?		X
Hlídá areál bezpečnostní služba?	X	
Provádí bezpečnostní služba kontrolu osob, vozidel a nákladů na vrátnici?		X
Probíhá v pracovní dny evidence osob při jejich vstupu do areálu?		X
Funguje bezpečnostní služba v rámci areálu nepřetržitě?		X
Dochází občas k náhodnému úniku při manipulaci s HK?	X	
Je areál, prostor kolem firmy i samotný sklad snímán kamerami?		X
Je spolehlivost, samostatnost a odbornost hlavním kritériem při výběru nových zaměstnanců?	X	
Absolvují noví zaměstnanci vstupní prohlídku u smluvního lékaře?		X
Provádějí se pravidelné kontroly znalostí z oblasti BOZP?	X	
Používají zaměstnanci při práci vhodné ochranné pomůcky?	X	
Jsou o předávání OOPP prováděny pravidelné zápisy?		X
Stal se za posledních 10 let pracovní úraz na pracovišti?		X
Je nákladní rampa zabezpečena proti pádu z ní zábradlím?		X

Jsou prostory firmy a nákladní auta vybaveny vhodnými prostředky požární ochrany?	X	
Je ustanovena v rámci společnosti požární preventivní hlídka?	X	
Je dodržována požární prevence ze strany všech zaměstnanců?		X
Provádí pravidelné kontroly dodržování podmínek požární bezpečnosti odborně způsobilá osoba?	X	
Jsou o těchto kontrolách všechny zápisy v Požární knize?		X
Byl zjištěn nedostatek v umístění bezpečnostních tabulek?	X	
Je dodržen vymezený prostor pod všemi plynovými jednotkami ROBUR?		X
Byla za poslední rok provedena kontrola plynových zařízení?		X
Má firma vypracován provozní řád a vede provozní deník na plynové zařízení?		X
Byla provedena za poslední rok revize elektrických spotřebičů?		X
Byla obsluha plynových zařízení dostatečně zaškolená a je písemně pověřena?		X
Existuje interní směrnice pro oblast informační bezpečnosti?		X
Jsou informační systémy chráněny proti virům?	X	
Je přístup do programu kontrolován pomocí identifikace uživatelů?	X	

Pomocí metody Kontrolní seznam byly identifikovány tyto hrozby:

- překonání plotů a vniknutí do areálu,
- nepřehlednost o pohybu osob po areálu,
- krádež materiálu, výrobků,
- zneužití času bez výkonu strážní služby,
- vniknutí do areálu,
- vniknutí do objektu velkoobchodu,
- zneužití klíčů zaměstnanci společnosti,
- zranění při opouštění objektu v případě požáru,
- požár z důvodu neodstraněných případně zjištěných závad,
- neodborná kontrola plynových zařízení,
- neodpovědnost za kontroly plynových zařízení,
- neznalost v oblasti plynových zařízení,
- požár z důvodu neodstraněných případně zjištěných závad,
- požár z důvodu náhodného úniku HK,
- nedodržení volného vymezeného prostoru,

- není přístup k jednotce v případě potřeby,
- pád nebo pracovní úraz,
- zdravotní nezpůsobilost k výkonu práce zaměstnanců,
- nepřehlednost, zvýšené náklady na OOPP,
- požár z důvodu špatného stavu elektrických spotřebičů,
- neznalost v oblasti informační bezpečnosti, únik informací.

7.4.3 Analýza rizik pomocí metody polo-kvantitativní metody „PNH“

Pro komplexní posouzení a ohodnocení rizik byla zvolena polo-kvantitativní metoda PNH.

Pomocí této metody jsou rizika vyhodnocena ve třech složkách, a to s ohledem na:

- pravděpodobnost vzniku hrozby - **P**,
- závažnost následků - **N**,
- názor hodnotitelů – **H**.

Všechny tři složky jsou určeny odhadem.

Odhad pravděpodobnosti vzniku hrozby P je stanoven podle stupnice pravděpodobnosti vzestupně číslem 1–5, jak je vidět v tabulce č. 12.

Tab. 12. Stupnice pravděpodobnosti vzniku hrozby [14]

Pravděpodobnost vzniku hrozby	Číselné vyjádření
Téměř nulová	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Trvalá	5

Pravděpodobnost následků, tedy závažnost N, je vyjádřena stejně pomocí číselného ohodnocení 1–5, - viz tabulka č. 13.

Tab. 13. Stupnice závažnosti následků [14]

Závažnost následků	Číselné vyjádření
Bez následků	1
Mírná závažnost	2
Větší závažnost	3
Velká závažnost	4
Katastrofický následek	5

Názor hodnotitelů H zohledňuje míru závažnosti ohrožení pomocí bodové stupnice 1–5, viz tabulka č. 14.

Tab. 14. Stupnice názoru hodnotitelů [14]

Míra závažnosti ohrožení	Číselné vyjádření
Zanedbatelný vliv	1
Mírný vliv	2
Větší nezadatelný vliv	3
Velký a významný vliv	4
Kritický vliv	5

Celkové hodnocení rizika je získáno součinem jednotlivých činitelů, výsledkem je ukazatel míry rizika $R = P \times N \times H$.

Jednotlivé rizikové stupně jsou vidět v tabulce č. 15.

Tab. 15. Rizikový stupeň [14]

Rizikový stupeň	Míra rizika ohodnocená slovně	R
I.	Nepříjatelné	≥ 100
II.	Nežádoucí	50-99
III.	Mírné	21-49
IV.	Akceptovatelné	6-20
V.	Bezvýznamné	< 5

Metoda PNH je zpracována do tabulky č. 16.

Tab. 16. Metoda PNH [14]

Hrozba	P	N	H	R
Překonání plotu a vniknutí do areálu	4	3	3	36
Vniknutí do areálu	2	3	4	24
Krádež materiálu, výrobků	3	2	2	12
Nepřehlednost o pohybu osob a aut	3	2	3	18
Zneužití času bez výkonu strážní služby	3	3	3	27
Vniknutí do objektu velkoobchodu	2	3	4	24
Nepřehlednost v klíčovém režimu - zneužití klíčů zaměstnanci společnosti	2	2	2	8
Zranění při opouštění objektu v případě požáru	4	4	4	64
Požár z důvodu neodstraněných případně zjištěných závad v oblasti PO	2	4	4	32
Pád – pracovní úraz	2	3	3	18
Nepřehlednost o předávání OOPP zaměstnancům, zvýšené náklady	2	2	1	4
Zdravotní nezpůsobilost k výkonu práce zaměstnanců	2	2	1	4
Nedodržení vymezeného prostoru	4	2	3	24

Špatný přístup k plynové jednotce	4	2	3	24
Požár při náhodném úniku HK	1	4	4	16
Požár z důvodu špatného stavu elektrických spotřebičů	2	4	4	32
Požár z důvodu neodstraněných případně zjištěných závad na plynovém zařízení	2	4	4	32
Neznalost v oblasti plynových zařízení	4	4	4	64
Neodborná kontrola plynového zařízení	3	4	4	48
Neodpovědnost za kontroly plynových zařízení	3	3	3	27
Neznalost v oblasti informační bezpečnosti, únik informací	2	4	3	24

Metodou PNH byla zjištěna rizika v rizikových stupních II., III., IV. a V.

Pro distribuční společnost jsou nejzávažnější 2 hrozby s rizikovým stupněm II.:

- zranění při opuštění objektu při požáru,
- neprováděné kontroly a revize na plynovém zařízení.

7.5 Vyhodnocení silných míst a nedostatků v jednotlivých oblastech bezpečnosti

Pro přehlednost a shrnutí jsou zpracována silná místa a nedostatky v jednotlivých oblastech bezpečnosti v distribuční společnosti.

7.5.1 Obvodová ochrana areálu

Silná místa: Celý komplex areálu pochází ze sedmdesátých let 20. století a v minulých letech jeho majitelé do něho mnoho neinvestovali. Naštěstí s výměnou vedení areálu dochází k postupnému zlepšování a modernizaci. V minulém roce byla vyměněna kovová vstupní brána do areálu, nyní je z pevnějšího a odolnějšího materiálu.

Zjištěné nedostatky: Ploty jsou různých výšek 1,5–2 m, některé úseky jsou ve špatném technickém stavu a bez ostnatého drátu. Za budovou distribučního skladu je plot vysoký pouze 1,5 m a bez ostnatého drátu, podle mého úsudku je velmi dobře překonatelný

ve večerních hodinách. Proto je oplocení z mého pohledu jedno z nejzranitelnějších míst celého areálu.

Dalším nedostatkem je scházející kamerový systém, který by vhodně doplnil fyzickou ostrahu, monitoroval by kritická místa, pohyb osob a aut po areále a zvýšil celkovou bezpečnost v areále.

7.5.2 Kontrolní propustková služba

Silná místa: Kladem je režim po uzavření brány, ve večerních a nočních hodinách, tedy v časovém intervalu 20:00–5:30. Vstup do areálu je povolen až po řádné evidenci osoby.

Zjištěné nedostatky: Nedostatkem v této oblasti je to, že zaměstnanci externí bezpečnostní služby nevykonávají prohlídku osob ani nákladu.

Dalším nedostatkem je to, že pohyb osob a aut po areálu v čase, kdy je hlavní brána otevřena – tedy 5:30–20:00, je zcela volný, bez jakékoliv evidence.

7.5.3 Fyzická ostraha

Silná místa: O víkendech pracují zaměstnanci externí bezpečnostní agentury v nepřetržitém provozu. Úkony, které mají pro areál zajišťovat, jsou provedeny v pořádku a dostatečně.

Zjištěné nedostatky: Ve dnech pondělí až pátek nefunguje fyzická ostraha ve 24 hodinovém režimu, ale pouze ve vymezeném čase, tedy v časovém rozmezí 14:00–06:00, což je nedostatečné.

7.5.4 Plášťová ochrana

Silná místa: Před dvěma roky proběhla výměna vstupních dveří a oken, což zvýšilo bezpečnost budovy.

Zjištěné nedostatky: V rámci ochrany celého objektu není bohužel nainstalován kamerový systém, který by monitoroval pohyb osob na zranitelných místech a vhodně doplnil externí fyzickou ostrahu.

7.5.5 Klíčový režim

Silná místa: Klíčový režim je zaměstnanci společnosti dodržován i bez písemné interní směrnice. Strážníci si vedou pravidelné záznamy o předávání klíčů do deníku.

Zjištěné nedostatky: Schází interní směrnice pro klíčový režim, kde by bylo přesně definováno, kdo má od jakých dveří klíče a kdy je možno vstupovat do objektu.

7.5.6 Požární ochrana

Silná místa: Požární ochraně je věnována velká pozornost, probíhají pravidelné měsíční kontroly externí osobou způsobilou v PO, zaměstnanci absolvují školení ve stanovených termínech, je ustanovena požární hlídka v rámci společnosti.

Zjištěné nedostatky: V rámci požární prevence je potřeba udržovat volné únikové cesty, což na jednom místě nebylo splněno. Jedna polovina kovových vrat uvnitř skladu byla zaskládána paletou se zbožím, což znemožňuje jejich úplné otevření.

Dále bylo zjištěno, že v požární knize schází jeden zápis o provedené kontrole osobou způsobilou v PO. Kontrola podle zjištění u vedoucího střediska proběhla v pořádku bez nedostatků, ale nebyl učiněn záznam.

7.5.7 BOZP

Silná místa: Společnost má pro oblast BOZP zpracovanou interní směrnici, jsou dodržovány termíny pravidelných školení zaměstnanců. Zaměstnancům jsou předávány vhodné OOPP, zápis o předání probíhá na Evidenční listy a průběžně je kontrolováno jejich používání. Společnost má smlouvu s lékařem o pracovně-lékařské službě, který zajišťuje vstupní a preventivní prohlídky zaměstnanců.

Zjištěné nedostatky: V oblasti BOZP bylo zjištěno v rámci interního auditu nejvíce nedostatků.

Nákladová rampa nemá bezpečnostní zábradlí, které by bránilo pádu z rampy při manipulaci se zbožím.

Vhodné OOPP jsou sice zaměstnancům předávány ve stanovených intervalech, ale u tří zaměstnanců schází zápis v Evidenčním listě.

U dvou nových zaměstnanců chybí vstupní zdravotní prohlídka u smluvního lékaře.

Při manipulaci s HK dochází, i když minimálně, k náhodnému úniku HK na podlahu skladu.

Pod vytápěcími plynovými jednotkami ROBUR je sice prostor, který má zůstat volný označen na podlaze skladu žlutou čarou, ale schází zde bezpečnostní tabulky „Vymezený prostor musí zůstat volný“.

U jedné jednotky ROBUR je tento vymezený prostor zaskládán zbožím.

Schází revize na elektrické spotřebiče za poslední rok.

Chybí kontrola plynových zařízení za rok 2017 odbornou osobou.

Společnost nemá zpracovaný provozní řád na plynová zařízení dle ČSN 38 6405 a schází provozní deník.

Obsluha plynových zařízení byla poučena o obsluze těchto zařízení odbornou osobou pouze ústně a v krátkosti, schází kompletní zaškolení a následný záznam o tomto školení.

Určený zaměstnanec vykovává obsluhu plynových zařízení na základě ústní dohody, nemá písemné pověření ze strany společnosti.

7.5.8 Informační bezpečnost

Silná místa: Implementace jednotného IS do společností napříč skupinou proběhla úspěšně, systém je plně funkční a naplnila se očekávání majitelů o úspoře nákladů a zvýšení efektivnosti práce. V minulém roce proběhla obnova všech PC a tiskáren na středisku. Serverovna, která se nachází mimo budovu distribuční společnosti je zabezpečena dostatečně. V nočních hodinách probíhá pravidelné zálohování dat. Všechny pracovní stanice jsou kvůli nenadálému výpadku elektrického proudu napojeny na záložní UPS. Na všech PC je nainstalován antivirový program. Uživatelé se přihlašují do IS pomocí svého uživatelského jména a hesla. Obměna hesel probíhá každé tři měsíce. Práva do IS jsou zaměstnancům omezeny na základě principu „nutná potřeba k práci“.

Zjištěné nedostatky: V rámci oblasti informační bezpečnosti není zpracována interní směrnice. Informace o používání PC, pravidelné změně hesla k přístupu do IS, o nakládání s informacemi předává zaměstnancům pouze ústně vedoucí střediska nebo v případě potřeby upřesnění vedoucí IT oddělení.

7.6 Závěry auditu

V rámci interního auditu v distribuční společnosti byl hodnocen nastavený systém bezpečnosti. Audit se týkal následujících oblastí:

Obvodová ochrana areálu, kontrolní propustková služba, fyzická ostraha, plášťová ochrana budovy skladu, klíčový režim firmy, požární ochrana, BOZP a informační bezpečnost.

Je vidět, že společnost s riziky pracuje a snaží se jim předcházet. Přesto v každé z těchto oblastí byl zjištěn nedostatek, ale jejich závažnost není pro společnost nepřijatelná. **Proto je celkové hodnocení auditu, že nastavený bezpečnostní systém vyhovuje s výhradou.**

Zvolenou metodou analýzy rizik byly ohodnoceny potencionální hrozby. Byla zjištěna rizika v rizikových stupních II., III., IV. a V. Doporučení pro distribuční společnost je následující:

Rizika II. stupně – tato rizika vyžadují urychlené provedení odpovídajícího opatření, aby bylo riziko sníženo na přijatelnou úroveň.

Rizika III. stupně – nejsou tak ohrožující jako stupeň II., ale je třeba realizovat navržená bezpečnostní opatření.

Rizika IV. stupně – rizika jsou přijatelná se souhlasem vedení společnosti, ke snížení těchto rizik postačí zavedení vhodných organizačních opatření, běžný dozor a školení zaměstnanců.

Rizika V. stupně – je to bezvýznamné riziko pro společnost, ale je potřeba na něho upozornit. Postačí realizace organizačních opatření.

Na základě této analýzy jsou v tabulce č. 17 navržena klíčová bezpečnostní opatření, která by po jejich přijetí ve společnosti měla rizika minimalizovat na přijatelnou úroveň.

Tab. 17. Tabulka s návrhem klíčových bezpečnostních opatření [14]

Číslo	Hrozba	Opatření
1	Překonání plotu a vniknutí do areálu	Sjednocení výšky plotů, výměna poškozených částí plotů
2	Vniknutí do areálu	Instalace kamerového systému v rámci areálu
3	Krádež materiálu, výrobků	Namátkové kontroly osob a nákladu přes týden, o víkendu automaticky s evidencí osob.

4	Nepřehlednost o pohybu osob a aut	Evidence osob na vrátnici
5	Zneužití času bez výkonu strážní služby	Nepřetržitý provoz pro zaměstnance bezpečnostní agentury
6	Vniknutí do objektu velkoobchodu	Instalace kamerového systému na budovu skladu
7	Nepřehlednost v klíčovém režimu - zneužití klíčů zaměstnanci společnosti	Vypracování směrnice pro klíčový režim
8	Zranění při opuštění objektu v případě požáru	Přemístnění palety, poučení zaměstnanců o důležitosti požární prevence
9	Požár z důvodu neodstraněných případně zjištěných závad v oblasti PO	Doplnit záznam o kontrole PO a odstranit případné nedostatky
10	Pád – pracovní úraz	Montáž zábradlí podél celé rampy
11	Nepřehlednost o předávání OOPP zaměstnancům, zvýšené náklady	Doplnit zápisy, zajistit podpisy zaměstnanců
12	Zdravotní nezpůsobilost k výkonu práce zaměstnanců	Zajistit vstupní prohlídky u smluvního lékaře
13	Nedodržení vymezeného prostoru	Nainstalovat bezpečnostní tabulky „Vymezený prostor musí zůstat volný“
14	Špatný přístup k plynové jednotce	Prostor pod ROBUREM uvolnit, poučit zaměstnance
15	Požár při náhodném úniku HK	Poučení zaměstnanců o vhodné manipulaci s HK a požární prevenci
16	Požár z důvodu špatného stavu elektrických spotřebičů	Zajistit revizi u odborné osoby, dodržovat termín revize

17	Požár z důvodu neodstraněných případně zjištěných závad na plynovém zařízení	Zajistit kontrolu u odborné osoby, odstranit případné nedostatky, dodržovat termín kontrol
18	Nepřehlednost v oblasti plynových zařízení	Zajistit vypracování provozního řádu na plynové zařízení u odborné osoby
19	Neodborná kontrola plynového zařízení	Zajistit proškolení, záznam o tomto školení
20	Neodpovědnost za kontroly plynových zařízení	Písemné pověření určeného zaměstnance pro obsluhu plynových zařízení
21	Nepřehlednost v oblasti informační bezpečnosti, únik informací	Vypracování interní směrnice

Na základě zjištěných nedostatků během auditu doporučuji vedení společnosti provést následující opatření. Pro přehlednost jsou tato opatření seřazena podle rizikových stupňů, tedy podle naléhavosti k zavedení opatření:

1. V rámci požární prevence udržovat volné únikové cesty a paletu se zbožím, která brání plnému otevření vrat ve skladě, přemístit na jiné vhodné místo. Dále doporučuji znovu proškolit skladníky odborně způsobilou osobou v PO o důležitosti této prevence a vedoucímu střediska, aby prováděl namátkové kontroly ve skladě.
2. Zajistit kontrolu na plynová zařízení u odborné osoby. Dále doporučuji dodržovat řádné termíny revizí a kontrol, jako vhodný nástroj je „Plán revizí, kontrol a školení pro daný rok. Návrh plánu je v příloze PI.
3. Ploty kolem celého areálu sjednotit na jednotnou výšku minimálně 2 m a doplnit o čtyři prameny ostnatého drátu, jako ochranou před vniknutím. Úseky plotu, které jsou ve špatném technickém stavu, vyměnit za nové, funkční.
4. V rámci modernizace areálu a zvýšení jeho bezpečnosti navrhuji instalovat kamerový systém. Kamery navrhuji umístit na kritická místa, což jsou: prostor

kolem vstupní brány, administrativní budova s vrátnicí a dále na každou budovu v areále, pokud již nemá její vlastník vyřešen svým kamerovým systémem. Vhodné umístění kamer pro distribuční společnost bude řešeno v bodě č. 6.

5. V dnešní době, kdy se množství krádeží a vniknutí do objektů neustále zvyšuje, se mi zdá pracovní doba externí bezpečnostní agentury nedostačující. Doporučuji zavedení nepřetržitého provozu i přes pracovní dny. Strážní by tím pádem mohli provádět evidenci osob, namátkové kontroly osob a materiálu, častější kontrolní pochůzky po areále a obsluhu na dohledovém a poplachovém přijímacím centru, kam by byl posílán záznam z kamerového systému.
6. V rámci zvýšení bezpečnosti i objektu distribuční společnosti, doporučuji instalaci kamer na tyto kritická místa: vstupní dveře do administrativní části, 3 x kovová vrata do skladovacích prostorů a roh budovy administrativní části, která by zároveň snímala prostranství u nákladové rampy, kde parkují nákladní auta po návratu z rozvozových tras a přes víkend.
7. Kontaktovat externí osobu způsobilou v PO a požádat ji o doplnění chybějícího zápisu o pravidelné měsíční kontrole do požární knihy. Vedoucímu střediska, který se těchto kontrol zúčastňuje, doporučuji, aby po každé provedené kontrole zápis do požární knihy zkontroloval.
8. Žlutě označené vymezené prostory na podlaze skladu pod plynovými vytápěcími jednotkami ROBUR řádně označit bezpečnostní tabulkou „Vymezený prostor musí zůstat volný“. Tyto tabulky doporučuji umístit na zeď pod ROBURY do výšky 150 cm od podlahy, tedy do zorného pole.
9. Vymezený prostor pod 1 jednotkou ROBUR vyklidit a znovu poučit zaměstnance o nutnosti dodržování tohoto prostoru ve volném stavu.
10. Opakovaně proškolit zaměstnance o správné manipulaci s HK a nutnosti dodržování požární prevence.
11. Zajistit revizi na elektrické spotřebiče u odborné osoby. Dále doporučuji odpovědné osobě kontrolovat termíny revizí.
12. Zajistit zpracování provozního řádu na plynová zařízení dle normy dle ČSN 38 6405 u odborné osoby. Dále doporučuji zavedení provozního deníku pro plynová zařízení. Návrh deníku je v příloze PII.
13. Zajistit řádné zaškolení obsluhy plynových zařízení u odborné osoby a následně provést o tomto školení záznam.

14. Po absolvování potřebného školení písemně pověřit obsluhu plynových zařízení a stanoveného zaměstnance řádně seznámit s jeho povinnostmi. Návrh písemného pověření je v příloze PIII.
15. Pověřit vedoucího zaměstnance IT oddělení vypracováním interní směrnice pro oblast informační bezpečnosti. Doporučuji zapracovat následující informace pro zaměstnance: Pravidla pro používání PC včetně přístupu na internet, zálohování dat, interval pro změnu hesla k přístupu do IS, nakládání s informacemi.
16. Pracovníci externí bezpečnostní agentury nemají v popisu práce provádění prohlídky osob ani nákladu. V rámci pracovního týdne, kdy se v areálu pohybují především zákazníci firem, které zde sídlí, doporučuji provádět namátkové kontroly. Po uzavření brány a ve víkendové dny, kdy je vstup do areálu omezen, doporučuji tyto kontroly provádět u všech osob a každého nákladu.
17. Pohyb osob a aut v areálu se neustále zvětšuje, proto doporučuji zavést evidenci těchto osob a aut i v době 5:30-20:00 v pracovní dny. Toto doporučení úzce souvisí s doporučením č. 5.
18. Vypracovat interní směrnici pro klíčový režim, kde by bylo přesně definováno, kdo má od jakých dveří klíče, kam se může vstupovat a v jakou dobu je vstup do objektu povolen.
19. V rámci prevence před pádem z nakládací rampy zajistit montáž snímatelného zábradlí podél celé její délky.
20. Doplnit chybějící zápisy o předání OOPP do evidenčního listu u tří zaměstnanců a zajistit jejich podpisy. Vedoucímu střediska, který je zodpovědný za předávání OOPP a zápisy do evidenčních listů, doporučuji provádět zápis zrovna po předání OOPP zaměstnanci.
21. Objednat vstupní lékařské prohlídky dvou nových zaměstnanců u smluvního lékaře pro pracovní-lekářskou činnost. Dále doporučuji tyto vstupní prohlídky provádět ihned po přijmutí nového zaměstnance, aby bylo posouzeno, zda je zdravotně způsobilý vykonávat danou práci.
22. Kontaktovat vedení areálu a seznámit je s výsledky provedeného auditu za oblast obvodové ochrany areálu, kontrolní propustkové služby a fyzické ostrahy, jelikož tyto oblasti jsou zabezpečovány z jejich strany, jako majiteli areálu. Dále je obeznámit s navrženými doporučení č. 3, 4, 5, 6, 16, 17, která by vedla k celkovému zvýšení bezpečnosti areálu.

23. Provádět bezpečnostní audit v pravidelných intervalech, provádět okamžité řešení pro odstranění rizik a provádět preventivní opatření před těmito riziky.

7.7 Shrnutí kapitoly

V této kapitole byl zpracován samotný interní audit v distribuční firmě. Po stanovení záměru auditu byla provedena analýza současného stavu a metodou Kontrolní seznam identifikovány hrozby. Jejich analýza byla provedena pomocí metody PNH. V závěru byly shrnuty nedostatky a silné místa, celkově zhodnocen výsledek auditu a následně navrženy doporučení, která by měla sloužit k minimalizaci rizik.

ZÁVĚR

Provedení bezpečnostního auditu v konkrétní společnosti je vhodný nástroj ke zjištění, na jakém stupni se bezpečnost ve firmě skutečně nachází. Se zjištěnými výsledky je třeba pracovat, navrhnout opatření zrealizovat, a tím snížit rizika na přijatelnou úroveň pro organizaci. Dalším nezbytným krokem by měla být následná kontrola.

Cílem diplomové práce bylo udělat bezpečnostní audit pro distribuční firmu. Na základě analýzy vstupních informací identifikovat hrozby a po analýze rizik navrhnout konkrétní bezpečnostní opatření.

V úvodní kapitole teoretické části jsou definovány základní pojmy z oblasti bezpečnosti a řízení rizik, jako je bezpečnost, aktivum, hrozba, riziko, analýza rizik nebo řízení rizik. Dále jsou stručně popsány metody analýzy rizik a zvolené metody Kontrolní seznam a PNH pro praktickou část diplomové práce. Ve druhé kapitole byl vysvětlen samotný pojem bezpečnostní audit, jaké jsou jeho cíle, možnosti dělení z různých hledisek, jeho jednotlivé oblasti a v neposlední řadě byly detailně popsány jednotlivé kroky BA. V závěru teoretické části je charakterizována obecně distribuční společnost, s jejich specifiky.

V rámci čtvrté kapitoly, kterou začíná praktická část, proběhlo seznámení s distribuční společností, ve které je proveden bezpečnostní audit. Bylo zmíněno její personální zajištění, organizační struktura a samotný prodejní sortiment.

V rámci páté kapitoly byl stručně popsán areál, ve kterém sídlí vybraný velkoobchod. Bylo popsáno, jak zde probíhá kontrolní propustková služba, fyzická ostraha i jakým způsobem je zabezpečen celý areál.

V šesté kapitole je blíže charakterizována budova distribuční společnosti a je popsán současný stav plášťové ochrany, klíčového režimu ve firmě, požární ochrany, BOZP a taky informační bezpečnosti

Ve stěžejní závěrečné kapitole byl zpracován samotný interní audit v distribuční společnosti. Nejdříve byl stanoven cíl a záměr auditu, následovala prohlídka a analýza současného stavu ve společnosti, analýza dokumentace a vnitropodnikových směrnic souvisejících s bezpečností. Metodou Kontrolní seznam byly identifikovány hrozby a pomocí metody PNH byla zjištěna rizika v rizikových stupních II., III., IV. a V., která jsou pro společnost různě kritická. Celkem bylo během auditu odhaleno 21 nedostatků, nejvíce jich bylo v oblasti BOZP. Byla zmíněna i silná místa. Výsledek bezpečnostního

audit je – **vyhovující s výhradou**. V závěru byla navržena bezpečnostní opatření, která by měla sloužit k minimalizaci rizik. Společnost by se měla nejdříve zaměřit na odstranění rizik II. stupně, která jsou pro ni nejzávažnější.

Dále bylo vedení společnosti doporučeno kontaktovat majitele areálu, ve kterém distribuční společnost sídlí, a seznámit je s výsledky provedeného auditu za oblast obvodové ochrany areálu, kontrolní propustkové služby a fyzické ostrahy, jelikož tyto oblasti jsou zabezpečovány z jejich strany, jako majiteli areálu. Dále je obeznámit s navrženými doporučení č. 3, 4, 5, 6, 15, 16, která by vedla k celkovému zvýšení bezpečnosti areálu.

Podle výsledků auditu je vidět, že společnost se snaží rizikům ve většině případů předcházet. Přesto je dobré provádět bezpečnostní audit v pravidelných intervalech, aby byl zjištěn momentální stav a bylo možné včas reagovat vhodným bezpečnostním opatřením na novou hrozbu. Vždy je lépe a levnější pro společnost rizikům předcházet, než pak odstraňovat jejich velké a drahé následky.

SEZNAM POUŽITÉ LITERATURY

- [1] LUKÁŠ, Luděk a kolektiv. *Bezpečnostní technologie, systémy management V.* Vyd.1. Zlín: Radim Bačuvčík – VeRBum, 2015, 368 s. ISBN 978-80-87500-67-5.
- [2] BRABEC, František. *Ochrana bezpečnosti podniku.* Vyd. 1. Praha: EUROUNION, s.r.o., 1996, 203 s. ISBN 80-85858-29-0.
- [3] LUKÁŠ, Luděk a kolektiv. *Bezpečnostní technologie, systémy management II.* Vyd.1. Zlín: Radim Bačuvčík – VeRBum, 2012, 387 s. ISBN 978-80-87500-19-4.
- [4] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích.* 4., aktualiz. a rozš. vyd. Praha: GradaPublishing, 2013, 483 s. ISBN 978-80-247-4644-9
- [5] ŠEFČÍK, Vladimír. *Analýza rizik.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 98 s. ISBN 978-807-3186-968
- [6] SEILER, Milan. *Bezpečnostní audit v organizaci.* Praha: Soukromá vysoká škola ekonomických studií, 2014, ISBN 80-86744-20-5.
- [7] HROMADA, Martin. *Speciální technologie komerční bezpečnosti.* Prezentace. Zlín, 2018.
- [8] BRABEC, František a kolektiv. *Bezpečnost pro firmu, úřad, občana.* Praha: Public History, 2001, 400 s. ISBN 80-86445-04-06.
- [9] PZTS – poplachový a tísňový systém. *Security Guide.*[online]. 2018[cit. 2018-03-21]. Dostupné z <https://www.securityguide.cz/pzts-poplachovy-zabezpecovaci-a-tisnovy-system/>
- [10] Systémy přivolání pomoci pro seniory a nemohoucí. *Zabezpečovací-zařízení.* [online]. 2018[cit. 2018-03-21]. Dostupné z https://www.zabezpecovaci-zarizeni.cz/GSM-system-privolani-pomoci-seniorum/?utm_source=seznam&utm_medium=cpc&utm_campaign=VYH+SCP+syst%03%a9my&utm_content=SOS+t%03%ads%05%88ov%03%a9+tla%04%8d%03%adtko
- [11] KAMENÍK, Jiří a kolektiv. *Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur.* Vyd. 1. Praha: ASPI, a.s., 2007, 340 s. ISBN 978-80-7357-309-6

- [12] Zákon č.262/2006 Sb. Zákon zákoník práce. *Zákony pro lidi*. [online]. 2018 [cit. 2018-03-22]. Dostupné z: https://www.zakonyprolidi.cz/nabidka/cs/2006-262/zneni-20070101#p395_p395-9
- [13] Přilba ALPINWOLKER WR. *Flopp*. [online]. 2018 [cit. 2018-03-22]. Dostupné z: <http://prilby.flopp.cz/prilba-alpinworker-wr/pp/250/2453>
- [14] 246/2001 SB. VYHLÁŠKA O POŽÁRNÍ PREVENCI. *Zákony pro lidi*. [online]. 2018 [cit. 2018-03-22]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2001-246>
- [15] BRABEC, František a kolektiv. *Hlídací služby*. Praha: EUROUNION, spol. s r.o., 1995, 259 s. ISBN 80-85858-12-6
- [16] SELECKÝ, Matúš. *Penetrační testy a exploitace*. 1.vyd. Brno: ComputerPress, 2012, 303 s. ISBN 978-80-251-3752-9.
- [17] Penetrační testy. *AEC.CZ*. [online]. 2018 [cit. 2018-03-22]. Dostupné z: <https://www.aec.cz/cz/pentesty>
- [18] SIXTA, Josef. *Logistika: teorie a praxe*. Vyd. 1. Brno: CP Books, 2005, 315 s. Praxe manažera (CP Books). ISBN 80-251-0573-3.
- [19] SVĚTLÍK, Jaroslav. *Marketing - cesta k trhu*. Plzeň: Aleš Čeněk, 2005. ISBN 8086898482.
- [20] JAKUBÍKOVÁ, D. *Strategický marketing*. Praha: Grada Publishing a.s., 2008. ISBN 978-80-247-2690-80.
- [21] HANÁKOVÁ, Bohdana. *Analýza rizik v distribuci*. Uherské Hradiště, 2016. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení Uherské Hradiště. Vedoucí práce Ing. Martin Hart, Ph.D.
- [22] Ploty, obložení. *Colorlak*. [online]. 2018 [cit. 2018-03-22]. Dostupné z: <https://www.colorlak.cz/sortiment/ploty-oblozeni>
- [23] Interiérové barvy. *Het*. [online]. 2018 [cit. 2018-03-22]. Dostupné z: <https://www.het.cz/cs/interierove-barvy/disperzni-oteruvzdorne/klasik/product.html?id=3>
- [24] Výrobky. *Spokar*. [online]. 2018 [cit. 2018-03-22]. Dostupné z: <http://www.spokar.com/cz/vyrobky/?id=487-stetec-plochy-81215.html>

- [25] Zámek visací 50 mm. *Světluška* [online]. 2018 [cit. 2018-03-22]. Zámek visací 50 mm. Dostupné z: <http://eshop.svetluska.cz/zamek-visaci-50mm-kovovy>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AR - Analýza rizik

BA - Bezpečnostní audit

BOZP - Bezpečnost a ochrana zdraví při práci

ČR - Česká republika

FO - Fyzická ochrana

HK - Hořlavé kapaliny

HS - Hadicový systém

IS - Informační systém

IT - Informační technologie

MZP - Mechanické zábranné prostředky

OOPP - Osobní ochranné pracovní pomůcky

PC - Počítač

PO - Požární ochrana

PZTS - poplachový zabezpečovací a tísňový systém

SEZNAM OBRÁZKŮ

<i>Obr. 1. Členění hrozeb do kategorií [3]</i>	14
<i>Obr. 2. Proces řízení rizik ve firmě[4]</i>	19
<i>Obr. 3. Technický bezpečnostní prostředek – mechanický [7]</i>	23
<i>Obr. 4. Technický bezpečnostní prostředek – elektronický [7]</i>	24
<i>Obr. 5. Ochranný prostředek při práci – přilba [7]</i>	29
<i>Obr. 6. Penetrační test v organizaci a jeho cíle [16]</i>	33
<i>Obr. 7. Cyklus auditu [7]</i>	34
<i>Obr. 8. Organizační struktura společnosti [zdroj vlastní]</i>	42
<i>Obr. 9. Prodejní sortiment [22][23][24]</i>	44
<i>Obr. 10. Vjezd do areálu [zdroj vlastní]</i>	45
<i>Obr. 11. Ukázka plotu s ostnatým drátem [zdroj vlastní]</i>	46
<i>Obr. 12. Ukázka plotu z jiné části areálu [zdroj vlastní]</i>	47
<i>Obr. 13. Vrátnice v administrativní budově [zdroj vlastní]</i>	47
<i>Obr. 14. Průmyslová teplovzdušná plynová jednotka ROBUR F1 [zdroj vlastní]</i>	51
<i>Obr. 15. Nákladová rampa [zdroj vlastní]</i>	52
<i>Obr. 16. Zámek visací 50mm</i>	52
<i>Obr. 17. Okna do skladu [zdroj vlastní]</i>	53
<i>Obr. 18. Požární kniha [zdroj vlastní]</i>	55
<i>Obr. 19. Označení skladu bezpečnostními tabulkami [zdroj vlastní]</i>	55
<i>Obr. 20. Práškové hasicí přístroje v nezatepleném skladu [zdroj vlastní]</i>	57
<i>Obr. 21. Požární hydrant [zdroj vlastní]</i>	58
<i>Obr. 22. Ovládací skříňka HS [zdroj vlastní]</i>	59
<i>Obr. 23. Záložní zdroj k PC [zdroj vlastní]</i>	65

SEZNAM TABULEK

Tab. 1. Kontrolní seznam – pracovní list [zdroj vlastní]	18
Tab. 2. Pracovní doba strážných [zdroj vlastní]	49
Tab. 3. Přehled o umístění výstražných a bezpečnostních tabulek [zdroj vlastní]	56
Tab. 4. Přehled přenosných hasicích přístrojů [zdroj vlastní]	57
Tab. 5. Intervaly školení zaměstnanců o PO [zdroj vlastní]	59
Tab. 6. Povinnosti členů požární preventivní hlídky [zdroj vlastní]	60
Tab. 7. Seznam poskytovaných OOPP dle druhu pracovních činností a jejich životnost [zdroj vlastní]	61
Tab. 8. Evidenční list pro poskytování OOPP [zdroj vlastní]	62
Tab. 9. Seznam prověřených dokumentů a interních směrnic [zdroj vlastní]	67
Tab. 10. Přehled o provedení analýzy auditovaných oblastí [zdroj vlastní]	68
Tab. 11. Kontrolní seznam [zdroj vlastní]	69
Tab. 12. Stupnice pravděpodobnosti vzniku hrozby [zdroj vlastní]	71
Tab. 13. Stupnice závažnosti následků [zdroj vlastní]	72
Tab. 14. Stupnice názoru hodnotitelů [zdroj vlastní]	72
Tab. 15. Rizikový stupeň [zdroj vlastní]	73
Tab. 16. Metoda PNH [zdroj vlastní]	73
Tab. 17. Tabulka s návrhem klíčových bezpečnostních opatření [zdroj vlastní]	78

SEZNAM PŘÍLOH

PI Plán revizí, kontrol a školení pro rok 2019

PII Návrh provozního deníku pro plynová zařízení

PIII Návrh písemného pověření pro obsluhu plynových zařízení

**PŘÍLOHA P I: PLÁN REVIZÍ, KONTROL A ŠKOLENÍ PRO ROK
2019**

PLÁN REVIZÍ, KONTROL A ŠKOLENÍ PRO ROK 2019		
Typ revize, kontroly, školení	Termín	Datum splnění
Školení BOZP	1/2019	
Školení PO	2/ 2019	
Revize elektrospotřebičů, strojního zařízení	2/2019	
Kontrola plynového zařízení	3/2019	
Kontrola teplovzdušných agregátů ROBUR	5/2019	
Revize elektroinstalace	6/2019	
Revize hromosvodů	6/2019	
Kontrola hasicích přístrojů a hydrantů	9/2019	
Revizi ovládací skříňky HS	10/2019	
Školení řidičů	12/2019	

PŘÍLOHA P III: NÁVRH PÍSEMNÉHO POVĚŘENÍ PRO OBSLUHU PLYNOVÝCH ZAŘÍZENÍ

POVĚŘENÍ

Vedoucí střediska... jméno..... společnosti, se sídlem.....,

IČO:....., pověřuje zaměstnance, datum narození....., bytem.....,

PSČ:....., k obsluze plynových zařízení. Týká se to následujících úkonů:

- obsluha plynových spotřebičů,
- vizuální kontrola celého plynového zařízení,
- kontrola chodu spotřebičů a odtahů,
- kontrola funkce regulátoru a termostatů,
- kontrola těsnosti spojů,
- provádění zápisů do provozního deníku,
- nahlášení závad vedoucímu střediska.

V, dne.....

.....podpis vedoucího střediska.....

Jméno, funkce

.....podpis zaměstnance.....

Jméno zaměstnance